

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004852

International filing date: 11 March 2005 (11.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-074739  
Filing date: 16 March 2004 (16.03.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

11. 3. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 4 年 3 月 1 6 日

出 願 番 号  
Application Number: 特 願 2 0 0 4 - 0 7 4 7 3 9

パリ条約による外国への出願  
に用いる優先権の主張の基礎  
となる出願の国コードと出願  
番号

The country code and number  
of your priority application,  
to be used for filing abroad  
under the Paris Convention, is

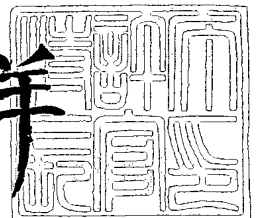
J P 2 0 0 4 - 0 7 4 7 3 9

出 願 人  
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 1 5 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川 洋



【書類名】 特許願  
【整理番号】 2048150045  
【提出日】 平成16年 3月16日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G09C 1/00  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 中野 稔久  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 大森 基司  
【特許出願人】  
    【識別番号】 000005821  
    【氏名又は名称】 松下電器産業株式会社  
【代理人】  
    【識別番号】 100090446  
    【弁理士】  
    【氏名又は名称】 中島 司朗  
【手数料の表示】  
    【予納台帳番号】 014823  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9003742

**【書類名】 特許請求の範囲****【請求項 1】**

同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、  
秘密鍵を生成する秘密鍵生成手段と、  
前記条件を特定するパラメータを複数取得するパラメータ取得手段と、  
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と  
を備えることを特徴とする情報セキュリティ装置。

**【請求項 2】**

前記情報セキュリティ装置は、ネットワークを介して複数のサーバ装置と接続されており、  
前記パラメータ取得手段は、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、  
前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成すること  
を特徴とする請求項 1 に記載の情報セキュリティ装置。

**【請求項 3】**

前記情報セキュリティ装置は、更に、  
前記公開鍵生成手段により生成された前記複数の公開鍵を、各公開鍵の生成に用いたパラメータの送信元であるサーバ装置へ送信する公開鍵送信手段と、  
前記複数のサーバ装置のそれぞれから、公開鍵及び各サーバ装置の署名を含む公開鍵証明書を取得する公開鍵証明書取得手段と、  
前記秘密鍵生成手段により生成された秘密鍵、及び、前記公開鍵証明書取得手段により取得された複数の公開鍵証明書を記憶する鍵記憶手段と  
を備えることを特徴とする請求項 2 に記載の情報セキュリティ装置。

**【請求項 4】**

前記情報セキュリティ装置は、更に、  
前記鍵記憶手段から一の公開鍵証明書を読み出し、読み出した公開鍵証明書を含むコンテンツ要求を、前記公開鍵証明書の発行元であるサーバ装置へ送信するコンテンツ要求手段と、  
前記秘密鍵及び前記公開鍵証明書に含まれる公開鍵とを用いて前記サーバ装置から安全かつ確実にコンテンツを取得するコンテンツ取得手段と  
を備えることを特徴とする請求項 3 に記載の情報セキュリティ装置。

**【請求項 5】**

前記コンテンツ取得手段は、  
前記秘密鍵を用いて生成した署名データを前記サーバ装置へ送信し、前記サーバ装置から前記公開鍵を用いて認証を受け、且つ、前記サーバ装置を認証する認証部と、  
前記認証部による認証に成功した場合に、前記サーバ装置と安全に鍵情報を共有する鍵共有部と、  
前記鍵情報を用いてコンテンツを暗号化した暗号化コンテンツを、前記サーバ装置から受信する受信部と、  
受信した暗号化コンテンツを前記鍵情報を用いて復号する復号部と  
を備えることを特徴とする請求項 4 に記載の情報セキュリティ装置。

**【請求項 6】**

前記鍵記憶手段は、当該情報セキュリティ装置に挿入された可搬型のメモリカードであって、  
前記公開鍵生成手段は、前記メモリカードに前記秘密鍵及び前記複数の公開鍵証明書を書き込み、  
前記メモリカードは、外部から解読及び改竄が不可能なセキュアな記憶領域を含み、前

記セキュアな記憶領域に前記秘密鍵を格納する

ことを特徴とする請求項 3 に記載の情報セキュリティ装置。

【請求項 7】

前記情報セキュリティ装置は、更に、

前記メモリカードが当該情報セキュリティ装置に挿入されると、前記メモリカードの正当性を認証するメモリカード認証手段と、

前記メモリカード認証手段による認証に失敗した場合、前記公開鍵生成手段による前記秘密鍵及び前記複数の公開鍵証明書の前記メモリカードへの書き込みを抑制する書込抑制手段と

を備えることを特徴とする請求項 6 に記載の情報セキュリティ装置。

【請求項 8】

前記情報セキュリティ装置は、楕円曲線上の離散対数問題を安全性の根拠とし、

前記パラメータ取得手段は、楕円曲線を構成するパラメータを複数取得し、

前記公開鍵生成手段は、取得した複数のパラメータごとに、前記秘密鍵に楕円曲線上の乗算を施すことにより、前記複数の公開鍵を生成する

ことを特徴とする請求項 1 に記載の情報セキュリティ装置。

【請求項 9】

前記秘密鍵生成手段は、1 個の秘密鍵  $SK$  を生成し、

前記パラメータ取得手段は、楕円曲線  $y^2 = x^3 + ax + b$  を構成するパラメータ  $a$ 、 $b$ 、素数  $p$ 、及び前記楕円曲線上の元  $G$  の組を複数取得し、

前記公開鍵生成手段は、取得した複数の組ごとに、 $SK * G \pmod{p}$  を計算することにより、前記複数の公開鍵を生成する

ことを特徴とする請求項 8 に記載の情報セキュリティ装置。

【請求項 10】

前記情報セキュリティ装置は、RSA 暗号を安全性の根拠とし、

前記秘密鍵生成手段は、1 個の秘密鍵  $d$  を生成し、

前記パラメータ取得手段は、前記パラメータとして、素数の組  $(P, Q)$  を複数取得し、

前記公開鍵生成手段は、取得した複数の素数の組ごとに、

$N = PQ$  を計算し、更に、 $ed \equiv 1 \pmod{(P-1)(Q-1)}$  から、 $e$  を計算し、前記複数の公開鍵  $(N, e)$  の組を生成する

ことを特徴とする請求項 1 に記載の情報セキュリティ装置。

【請求項 11】

同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱うメモリカードであって、

秘密鍵を生成する秘密鍵生成手段と、

前記条件を特定するパラメータを複数取得するパラメータ取得手段と、

取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と、

前記秘密鍵を、外部から解読及び改竄が不可能なセキュアな領域に記憶する秘密鍵記憶手段と

を備えることを特徴とするメモリカード。

【請求項 12】

前記メモリカードは、ネットワークを介して複数のサーバ装置と接続された端末に挿入されており、

前記パラメータ取得手段は、前記端末を介して、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、

前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成する

ことを特徴とする請求項 11 に記載のメモリカード。

**【請求項 13】**

前記メモリカードは、更に、  
前記秘密鍵及び前記複数の公開鍵を用いて、前記端末を介して、前記複数のサーバ装置それぞれから、安全かつ確実にコンテンツを取得することを特徴とする請求項 12 に記載のメモリカード。

**【請求項 14】**

同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティシステムであって、  
秘密鍵を生成する秘密鍵生成手段と、  
前記条件を特定するパラメータを複数個取得するパラメータ取得手段と、  
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と  
を備えることを特徴とする情報セキュリティシステム。

**【請求項 15】**

同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置で用いられる鍵生成方法であって、  
秘密鍵を生成する秘密鍵生成ステップと、  
前記条件を特定するパラメータを複数取得するパラメータ取得ステップと、  
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成ステップと  
を含むことを特徴とする鍵生成方法。

**【請求項 16】**

同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置で用いられる鍵生成プログラムであって、  
秘密鍵を生成する秘密鍵生成ステップと、  
前記条件を特定するパラメータを複数取得するパラメータ取得ステップと、  
取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成ステップと  
を含むことを特徴とする鍵生成プログラム。

【書類名】 明細書

【発明の名称】 情報セキュリティ装置及び情報セキュリティシステム

【技術分野】

【0001】

本発明は、安全かつ確実にコンテンツを送受信する技術に関する。

【背景技術】

【0002】

端末がコンテンツ配信業者のサービスを利用する場合、端末と、コンテンツ配信業者が有するサーバ装置とは、相互認証を行い、相互認証が成功した場合に安全に鍵を共有することにより安全な通信路、所謂 S A C (Secure Authentication Channel) を確立し、S A C を介してコンテンツを送受信する技術が特許文献 1 に開示されている。

【特許文献 1】 特開平 11 - 234259 号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

近年、コンテンツ配信サービスを提供する業者が増加してきており、1 台の端末で複数業者のサービスを利用する場合に対応できるシステムが要望されている。

そこで本発明は、1 台の端末で複数業者のサービスを利用するのに適した情報セキュリティ装置及び情報セキュリティシステムを提供することを目的とする。

【課題を解決するための手段】

【0004】

上記の目的を達成するために、本発明は、同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、秘密鍵を生成する秘密鍵生成手段と、前記条件を特定するパラメータを複数取得するパラメータ取得手段と、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段とを備えることを特徴とする。

【0005】

また、前記情報セキュリティ装置は、ネットワークを介して複数のサーバ装置と接続されており、前記パラメータ取得手段は、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成することを特徴とする。

また、前記情報セキュリティ装置は、更に、前記公開鍵生成手段により生成された前記複数の公開鍵を、各公開鍵の生成に用いたパラメータの送信元であるサーバ装置へ送信する公開鍵送信手段と、前記複数のサーバ装置のそれぞれから、公開鍵及び各サーバ装置の署名を含む公開鍵証明書を取得する公開鍵証明書取得手段と、前記秘密鍵生成手段により生成された秘密鍵、及び、前記公開鍵証明書取得手段により取得された複数の公開鍵証明書を記憶する鍵記憶手段とを備えることを特徴とする。

また、前記情報セキュリティ装置は、更に、前記鍵記憶手段から一の公開鍵証明書を読み出し、読み出した公開鍵証明書を含むコンテンツ要求を、前記公開鍵証明書の発行元であるサーバ装置へ送信するコンテンツ要求手段と、前記秘密鍵及び前記公開鍵証明書に含まれる公開鍵とを用いて前記サーバ装置から安全かつ確実にコンテンツを取得するコンテンツ取得手段とを備えることを特徴とする。

【0006】

また、前記コンテンツ取得手段は、前記秘密鍵を用いて生成した署名データを前記サーバ装置へ送信し、前記サーバ装置から前記公開鍵を用いて認証を受け、且つ、前記サーバ装置を認証する認証部と、前記認証部による認証に成功した場合に、前記サーバ装置と安全に鍵情報を共有する鍵共有部と、前記鍵情報を用いてコンテンツを暗号化した暗号化コンテンツを、前記サーバ装置から受信する受信部と、受信した暗号化コンテンツを前記鍵情報を用いて復号する復号部とを備えることを特徴とする。

**【0007】**

更に、上記目的を達成するための、本発明は、同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱うメモリカードであって、秘密鍵を生成する秘密鍵生成手段と、前記条件を特定するパラメータを複数取得するパラメータ取得手段と、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段と、前記秘密鍵を、外部から解読及び改竄が不可能なセキュアな領域に記憶する秘密鍵記憶手段とを備えることを特徴とする。

**【0008】**

また、前記メモリカードは、ネットワークを介して複数のサーバ装置と接続された端末に挿入されており、前記パラメータ取得手段は、前記端末を介して、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、前記公開鍵生成手段は、前記パラメータ取得手段が取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成することを特徴とする。

**【0009】**

また、前記メモリカードは、更に、前記秘密鍵及び前記複数の公開鍵を用いて、前記端末を介して、前記複数のサーバ装置それぞれから、安全かつ確実にコンテンツを取得することを特徴とする。

**【発明の効果】****【0010】**

本発明は、同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、秘密鍵を生成し、前記条件を特定するパラメータを複数取得し、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成することを特徴とする。

**【0011】**

この構成によると、情報セキュリティ装置は、秘密鍵から複数個の公開鍵を生成するため、秘密鍵と公開鍵とが1対1に対応している従来の装置と比較すると、複数個の公開鍵を生成する場合に、生成、管理する鍵の数が減るという効果がある。

ここで、前記情報セキュリティ装置は、ネットワークを介して複数のサーバ装置と接続されており、前記複数のサーバ装置から、それぞれ異なるパラメータを取得し、取得した複数のパラメータを用いて、それぞれ異なる前記複数の公開鍵を生成するように構成してもよい。

**【0012】**

この構成によると、情報セキュリティ装置は、複数のサーバ装置から、それぞれ異なるパラメータを取得することで、1個の秘密鍵から、複数個の異なる公開鍵を生成することができる。そのため、従来の装置が、通信を行うサーバ装置毎に1個の秘密鍵と1個の公開鍵とのペアを生成し、管理していたのと比較し、本発明の情報セキュリティ装置は、生成、管理する鍵の数が減るという効果がある。

**【0013】**

ここで、前記情報セキュリティ装置は、更に、生成した前記複数の公開鍵を、各公開鍵の生成に用いたパラメータの送信元であるサーバ装置へ送信し、前記複数のサーバ装置のそれぞれから、公開鍵及び各サーバ装置の署名を含む公開鍵証明書を取得し、生成した秘密鍵、及び、取得した複数の公開鍵証明書を記憶するように構成してもよい。

この構成によると、従来の装置は、通信を行うサーバ装置毎に1個の秘密鍵と1個公開鍵とのペアを記憶していたのと比較して、本発明の情報セキュリティ装置では、鍵記憶手段が記憶する鍵の数が減るので、記憶領域が削減され、コストの節減に繋がる。

**【0014】**

ここで、前記情報セキュリティ装置は、更に、記憶している複数の公開鍵証明書から、一の公開鍵証明書を読み出し、読み出した公開鍵証明書を含むコンテンツ要求を、前記公



開鍵証明書の発行元であるサーバ装置へ送信し、前記秘密鍵及び前記公開鍵証明書に含まれる公開鍵とを用いて前記サーバ装置から安全かつ確実にコンテンツを取得するように構成してもよい。

**【0015】**

この構成によると、情報セキュリティ装置は、記憶されている複数個の公開鍵証明書から、1個の公開鍵証明書を選ぶことで、1個の秘密鍵と選ばれた公開鍵証明書に含まれる公開鍵とを用いて、対応するサーバ装置からコンテンツをセキュアに取得することができる。

ここで、前記情報セキュリティ装置は、前記秘密鍵を用いて生成した署名データを前記サーバ装置へ送信し、前記サーバ装置から前記公開鍵を用いて認証を受け、且つ、前記サーバ装置を認証し、前記認証に成功した場合に、前記サーバ装置と安全に鍵情報を共有し、前記鍵情報を用いてコンテンツを暗号化した暗号化コンテンツを、前記サーバ装置から受信し、受信した暗号化コンテンツを、前記鍵情報を用いて復号するように構成してもよい。

**【0016】**

この構成によると、情報セキュリティ装置は、サーバ装置と相互認証を行い、その後、安全に鍵情報を共有することにより、サーバ装置と安全な通信路を確立することができる。

ここで、前記情報セキュリティ装置内の記憶装置は、当該情報セキュリティ装置に挿入された可搬型のメモリカードであって、前記情報セキュリティ装置は、前記メモリカードに前記秘密鍵及び前記複数の公開鍵証明書を書き込み、前記メモリカードは、外部から解読及び改竄が不可能なセキュアな記憶領域を含み、前記セキュアな記憶領域に前記秘密鍵を格納するように構成してもよい。

**【0017】**

この構成によると、情報セキュリティ装置内の記憶装置は、可搬型のメモリカードにより実現される。情報セキュリティ装置は、秘密鍵をメモリカードの耐タンパーモジュールに格納することにより、秘密鍵をセキュアに保持することができる。

ここで、前記情報セキュリティ装置は、更に、記メモリカードが当該情報セキュリティ装置に挿入されると、前記メモリカードの正当性を認証し、前記認証に失敗した場合、前記秘密鍵及び前記複数の公開鍵証明書の前記メモリカードへの書き込みを抑制するように構成してもよい。

**【0018】**

この構成によると、情報セキュリティ装置は、メモリカードの認証に成功した場合のみ、メモリカードに秘密鍵と公開鍵証明書とを書き込むので、不正なメモリカードに秘密鍵が書き込まれることにより秘密鍵が暴露されるのを防ぐことができる。

ここで、前記情報セキュリティ装置は、楕円曲線上の離散対数問題を安全性の根拠とし、楕円曲線を構成するパラメータを複数取得し、取得した複数のパラメータごとに、前記秘密鍵に楕円曲線上の乗算を施すことにより、前記複数の公開鍵を生成するように構成してもよい。また、前記情報セキュリティ装置は、1個の秘密鍵  $SK$  を生成し、楕円曲線  $y^2 = x^3 + ax + b$  を構成するパラメータ  $a$ 、 $b$ 、素数  $p$ 、及び前記楕円曲線上の元  $G$  の組を複数取得し、取得した複数の組ごとに、 $SK * G \pmod{p}$  を計算することにより、前記複数の公開鍵を生成するように構成してもよい。

**【0019】**

この構成によると、情報セキュリティ装置は、安全性の高い楕円曲線暗号を用いることで、安全かつ確実にコンテンツを取得することができる。

ここで、前記情報セキュリティ装置は、RSA暗号を安全性の根拠とし、1個の秘密鍵  $d$  を生成し、前記パラメータとして、素数の組  $(P, Q)$  を複数取得し、取得した複数の素数の組ごとに、 $N = PQ$  を計算し、更に、 $ed \equiv 1 \pmod{(P-1)(Q-1)}$  から、 $e$  を計算し、前記複数の公開鍵  $(N, e)$  の組を生成するように構成してもよい。

**【0020】**

この構成によると、情報セキュリティ装置は、公開鍵暗号方式としてRSA暗号を用いるため、本発明を、汎用のコンピュータシステムで実現することが可能である。

【発明を実施するための最良の形態】

【0021】

本発明に係る実施の形態として、情報セキュリティシステム1について説明する。情報セキュリティシステム1は、1台の端末で複数のコンテンツ配信業者が提供するサービスを利用するシステムである。

以下では、情報セキュリティシステム1について図面を参照して説明する。

<構成>

図1は、情報セキュリティシステム1の構成を示すシステム構成図である。同図に示す様に、情報セキュリティシステム1は、端末10、メモリカード20、サーバ装置30、サーバ装置40及びサーバ装置50から構成される。なお、メモリカード20は、端末10のメモリカードスロットに挿入して用いられ、端末10と、サーバ装置30、サーバ装置40及びサーバ装置50とは、ネットワーク60を介して接続されている。なお、ネットワーク60の具体例は、インターネットである。

【0022】

端末10及びメモリカード20は、コンテンツ配信サービスを利用する利用者が有する装置であり、サーバ装置30、サーバ装置40及びサーバ装置50は、それぞれ異なるコンテンツ配信業者が有する装置である。コンテンツ配信業者は、利用者に対して、コンテンツ配信サービスを提供する。

なお、端末10、メモリカード20、サーバ装置30、サーバ装置40及びサーバ装置50は、コンテンツを安全かつ確実に扱う装置であるので、これらの装置を情報セキュリティ装置と呼称することもある。

【0023】

1. 端末10

ここでは、端末10の構成について詳細に説明する。

図2は、端末10の構成を機能的に示す機能ブロック図である。同図に示す様に、端末10は、通信部101、操作入力部102、制御部103、メモリカード入出力部104、メモリカード認証部105、CRL格納部106、公開鍵暗号処理部107、記憶部108及び再生部109から構成される。

【0024】

端末10は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクドライブレユニット、ネットワーク接続ユニット、MPEGデコーダ、MPEGエンコーダ及びメモリカードスロット等から構成されるコンピュータシステムである。

(1) 通信部101

通信部101は、Webブラウザを備えるネットワーク接続ユニットであって、ネットワーク60を介してサーバ装置30、サーバ装置40及びサーバ装置50と接続されている。

【0025】

通信部101は、サーバ装置30からネットワーク60を介して情報を受信し、受信した情報を制御部103へ出力する。また、通信部101は、制御部103から情報を受け取り、受け取った情報をネットワーク60を介してサーバ装置30へ送信する。同様に、通信部101は、サーバ装置40からネットワーク60を介して情報を受信し、受信した情報を制御部103へ出力する。また、通信部101は、制御部103から情報を受け取り、受け取った情報をネットワーク60を介してサーバ装置40へ送信する。同様に、通信部101は、サーバ装置50からネットワーク60を介して情報を受信し、受信した情報を制御部103へ出力する。また、通信部101は、制御部103から情報を受け取り、受け取った情報をネットワーク60を介してサーバ装置50へ送信する。

【0026】

ここで、通信部101が各サーバ装置へ送信する情報の具体例は、サービス加入要求、

サービス利用要求、各サーバ装置とのSAC確立に用いる署名データ、鍵情報などである。また、通信部101が各サーバ装置から受信する情報の具体例は、各サーバ装置とのSAC確立に用いる署名データ、鍵情報、楕円曲線のシステムパラメータ、認証及び鍵共有処理の後に各サーバ装置から送信されるコンテンツ、などである。

#### 【0027】

更に、通信部101は、ネットワーク60を介して、認証局（以下、「CA（Certification Authority）」と呼称する）と接続されており、通信部101は、CAとの間で以下のように情報の送受信を行う。

通信部101は、CAから常に最新のCRL（Certification Revocation List）を受信し、受信した最新のCRLを、制御部103を介してCRL格納部106に格納する。CRLについては後述する。

#### 【0028】

通信部101は、制御部103を介して公開鍵暗号処理部107から公開鍵「PK\_\_0010」を受け取り、受け取った公開鍵をCAへ送信する。また、通信部101は、CAから公開鍵「PK\_\_0010」に対応する公開鍵証明書「Cert\_\_0010」を受信し、受信した公開鍵証明書を制御部103へ出力する。

ここで、本明細書において、「楕円曲線のシステムパラメータ」とは、楕円曲線 $E: y^2 = x^3 + ax + b$ を構成する $a$ 及び $b$ 、更に、素数 $p$ 、 $p$ の位数 $q$ 、楕円曲線 $E$ 上の任意の点（ベースポイント） $G$ を指すこととする。

#### （2）操作入力部102

操作入力部102は、利用者からの操作を受け付けるボタンなどを備える。操作入力部102は、利用者からの操作を受け付け、受け付けた操作に対応する操作信号を生成し、生成した操作信号を制御部103へ出力する。

#### 【0029】

ここで、操作信号の具体例は、サービス加入要求を示す信号、サービス利用要求を示す信号などである。

#### （3）制御部103

制御部103は、マイクロプロセッサ、ROM、RAMなどから構成され、マイクロプロセッサがコンピュータプログラムを実行することにより、制御部103は、以下に示す処理を行い、端末10の全体を制御する。

#### 【0030】

（a）制御部103は、メモ리카ード入出力部104から、メモ리카ード20の挿入を検知したことを示す信号を受け取ると、メモ리카ード認証部105に対して、メモ리카ード20の認証処理を行う指示を出力する。

（b）制御部103は、メモ리카ード認証部105から「認証OK」を示す信号を受け取ると、CAから公開鍵証明書の発行を受ける。より具体的には、制御部103は、公開鍵暗号処理部107から出力される公開鍵「PK\_\_0010」と予め内部に記憶している自身のデバイスID「ID\_\_0010」とを、通信部101を介してCAへ送信する。制御部103は、通信部101を介して公開鍵「PK\_\_0010」に対応する公開鍵証明書「Cert\_\_0010」をCAから受信し、受信した公開鍵証明書を、メモ리카ード入出力部104を介してメモ리카ード20へ出力する。

#### 【0031】

（c）制御部103は、操作入力部102から操作信号を受け取り、受け取った操作信号に応じた処理を行う。

例えば、制御部103は、操作入力部102から、サーバ装置30、サーバ装置40、又はサーバ装置50へのサービス加入要求を示す操作信号を受け取ると、メモ리카ード入出力部104に対して、メモ리카ード20から公開鍵証明書「Cert\_\_0010」を読み出す指示を出力し、更に、要求に対応するサーバ装置とSACを確立し、サービス加入処理を行う指示を、公開鍵暗号処理部107に出力する。

#### 【0032】

また、制御部 103 は、操作入力部 102 から、サーバ装置 30、サーバ装置 40 又はサーバ装置 50 へのサービス利用要求を示す操作信号を受け取ると、メモリカード入出力部 104 に対して、メモリカード 20 から、サービス用秘密鍵 SK 及び要求に対応するサーバ装置から受け取った公開鍵証明書を読み出す指示を出力し、更に、対応するサーバ装置と SAC を確立して、コンテンツを取得する指示を、公開鍵暗号処理部 107 に出力する。

#### 【0033】

(d) また、制御部 103 は、端末 10 とサーバ装置 30、サーバ装置 40、又はサーバ装置 50 とが SAC を確立した後、各サーバ装置との間で情報を送受信する際に、公開鍵暗号処理部 107 からセッション鍵を受け取り、受け取ったセッション鍵を暗号鍵又は復号鍵として用い、情報を暗号化してサーバ装置へ送信したり、サーバ装置から受信する暗号化された情報を復号したりする。

#### 【0034】

##### (4) メモリカード入出力部 104

メモリカード入出力部 104 は、メモリカードスロットを含み、メモリカードスロットに、メモリカード 20 が挿入されたことを検知すると、その旨を示す信号を制御部 103 へ出力する。また、メモリカード入出力部 104 は、メモリカード 20 が挿入されている状態において、制御部 103 とメモリカード 20 との間で情報の入出力を行う。

#### 【0035】

##### (5) メモリカード認証部 105

メモリカード認証部 105 は、マイクロプロセッサ、ROM、RAM などから構成され、前記 ROM 又は前記 RAM には、図 3 (a) に示すパスワードテーブル 120 が格納されている。

パスワードテーブル 120 は 1 以上のパスワード情報を含み、各パスワード情報は、メモリカード番号と認証用パスワードとを含む。メモリカード番号は、端末 10 に挿入して使用可能であるメモリカードを識別するための情報である。認証用パスワードは、対応付けられているメモリカード番号により識別されるメモリカードと端末 10 とが共有している情報であり、メモリカードの認証に用いられる 256 ビットデータである。

#### 【0036】

メモリカード認証部 105 は、制御部 103 から、メモリカード 20 がメモリカード入出力部 104 に挿入されたことを示す信号を受け取ると、パスワードテーブル 120 からメモリカード 20 に対応したパスワード情報 121 を読み出し、更に、パスワード情報 121 から認証用パスワード PW\_\_0 を読み出す。また、メモリカード認証部 105 は、56 ビットの乱数 R\_\_0 を生成する。

#### 【0037】

メモリカード認証部 105 は、生成した乱数 R\_\_0 を、制御部 103 及びメモリカード入出力部 104 を介してメモリカード 20 へ出力すると共に、乱数 R\_\_0 を暗号鍵として用い、認証用パスワード PW\_\_0 に暗号アルゴリズム E を施して暗号文 E1 を生成し、生成した暗号文 E1 を記憶する。なお、ここで用いられる暗号アルゴリズム E の一例は DES (Data Encryption Standard) である。

#### 【0038】

メモリカード認証部 105 は、制御部 103 及びメモリカード入出力部 104 を介してメモリカード 20 から暗号文 E2 を受け取ると、受け取った暗号文 E2 と記憶している暗号文 E1 とを比較する。E1 と E2 とが一致する場合、メモリカード認証部 105 は、「認証 OK」を示す信号を制御部 103 へ出力し、E1 と E2 とが一致しない場合、メモリカード認証部 105 は、「認証 NG」を示す信号を制御部 103 へ出力する。

#### 【0039】

##### (6) CRL 格納部 106

CRL 格納部 106 は、RAM で構成され、内部に CRL を格納している。CRL は、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器の ID が登録され

たリストである。

CRLは、CAにより管理されており、端末10は、ネットワーク60を介してCAからCRLを受信してCRL格納部106に格納する。ここで、端末10は、CAから常に最新のCRLを受信し、受信した最新のCRLをそれまで格納していたCRLに替えて、CRL格納部106に格納する。なお、以下では、CRL格納部106は、最新のCRLとして、図3(b)に示すCRL130を格納しているものとする。

#### 【0040】

また、CRLについては、「American National Standards Institute, American National Standard for financial Services, ANS X9.57: Public Key Cryptography For the Financial Industry: Certificate Management, 1997.」に詳しく開示されている。

#### (7) 公開鍵暗号処理部107

公開鍵暗号処理部107は、マイクロプロセッサ、ROM、RAM、乱数生成器などから構成される。

#### 【0041】

公開鍵暗号処理部107は、端末10がサーバ装置30、サーバ装置40及びサーバ装置50に対してサービス加入要求を行うとき、各サーバ装置との間でSACを確立する処理を行う。また、公開鍵暗号処理部107は、端末10がサーバ装置30、サーバ装置40及びサーバ装置50に対してサービス利用要求を行うとき、各サーバ装置との間でSACを確立する処理を行う。なお、ここで用いられる公開鍵暗号は、楕円曲線暗号及びRSA暗号である。

#### 【0042】

(楕円曲線上の離散対数問題)

ここでは、先ず、楕円曲線暗号の安全性の根拠として用いられる楕円曲線上の離散対数問題について簡単に説明する。

楕円曲線上の離散対数問題とは、 $E(GF(p))$ を有限体 $GF(p)$ 上で定義された楕円曲線とし、楕円曲線 $E$ の位数が大きな素数で割り切れる場合に、楕円曲線 $E$ に含まれる元 $G$ をベースポイントとする。このとき、楕円曲線 $E$ に与えられた元 $Y$ に対して、

$$Y = x * G$$

となる整数 $x$ が存在するならば、 $x$ を求めよ、という問題である。

#### 【0043】

ここで、 $p$ は素数、 $GF(p)$ は $p$ 個の元を持つ有限体である。また、この明細書において、記号「 $*$ 」は、楕円曲線に含まれる元を複数回加算する演算を示し、 $x * G$ は、次式に示すように、楕円曲線に含まれる元 $G$ を $x$ 回加算することを意味する。

$$x * G = G + G + G + \dots + G$$

離散対数問題を公開鍵暗号の安全性の根拠とするのは、多くの元を有する有限体 $GF(p)$ に対して、上記問題は極めて難しいからである。

#### 【0044】

なお、離散対数問題については、ニールコブリッツ著「アコースインナンバアセオリイアンドクリプトグラフィ」(Neal Koblitz, "A Course in Number theory and Cryptography", Springer-Verlag, 1987)に詳しく述べられている。

(楕円曲線の演算公式についての説明)

次に、楕円曲線の演算公式について、以下に説明する。

#### 【0045】

楕円曲線の方程式を

$$y^2 = x^3 + ax + b \text{ とし、}$$

任意の点 $P$ の座標を $(x_1, y_1)$ とし、任意の点 $Q$ の座標を $(x_2, y_2)$ とする。ここで、 $R = P + Q$ で定まる点 $R$ の座標を $(x_3, y_3)$ とする。

$P \neq Q$ の場合、 $R = P + Q$ は、加算の演算となる。加算の公式を以下に示す。

#### 【0046】

$$x_3 = \{ (y_2 - y_1) / (x_2 - x_1) \}^2 - x_1 - x_2$$

$$y_3 = \{ (y_2 - y_1) / (x_2 - x_1) \} (x_1 - x_3) - y_1$$

$P=Q$ の場合、 $R=P+Q=P+P=2 \times P$ となり、 $R=P+Q$ は、2倍算の演算となる。2倍算の公式を以下に示す。

$$x_3 = \{ (3x_1^2 + a) / 2y_1^2 - 2x_1$$

$$y_3 = \{ (3x_1^2 + a) / 2y_1 \} (x_1 - x_3) - y_1$$

なお、上記演算は、楕円曲線が定義される有限体上での演算である。また、楕円曲線の演算公式については、“Efficient elliptic curve exponentiation” (Miyaji, Ono, and Cohen著、Advances in cryptology-proceedings of ICICS'97, Lecture notes in computer science, 1997, Springer-verlag, 282-290.) に詳しく説明されている。

#### 【0047】

(サービス加入要求)

ここでは、端末10が、サーバ装置30に対してサービスへの加入を要求するときの公開鍵暗号処理部107について説明する。公開鍵暗号処理部107は、制御部103から乱数 $R_{0010}$ を受け取り、内部に記憶する。乱数 $R_{0010}$ は端末10自身の秘密鍵であり、SAC確立処理に用いられる。なお、乱数 $R_{0010}$ は、メモリカード20のセキュア領域に格納されており、制御部103がメモリカード入出力部104を介して読み出したものである。公開鍵暗号処理部107は、公開鍵暗号のアルゴリズムとしてRSA暗号を用い、サーバ装置30とSACを確立する。詳細については後述する。公開鍵暗号処理部107は、サーバ装置30との間で確立されたSACを用い、ネットワーク60、通信部101及び制御部103を介して、サーバ装置30から、楕円曲線のシステムパラメータ「 $a_1$ 、 $b_1$ 、 $p_1$ 、 $q_1$ 、及び、 $G_1$ 」を受け取る。

#### 【0048】

具体例として、 $a_1 = -3$

$$b_1 = 16461$$

$$p_1 = 20011$$

$$q_1 = 20023$$

$$G_1 = (1, 7553)$$

とする。

#### 【0049】

更に、公開鍵暗号処理部107は、サービス用秘密鍵SKを生成する。公開鍵暗号処理部107は、生成したサービス用秘密鍵SKとシステムパラメータとを用いて、公開鍵 $PK_A = SK * G_1 \pmod{p_1}$ を算出する。公開鍵暗号処理部107は、生成したSKを、制御部103及びメモリカード入出力部104を介してメモリカード20に格納し、算出した公開鍵 $PK_A$ を、サーバ装置30との間で確立されたSACを用い、制御部103、通信部101及びネットワーク60を介してサーバ装置30へ送信する。

#### 【0050】

次に、端末10が、サーバ装置40に対してサービスへの加入を要求するときの公開鍵暗号処理部107について説明する。公開鍵暗号処理部107は、制御部103から端末10自身の秘密鍵である乱数 $R_{0010}$ を受け取り、RSA暗号を用いて、サーバ装置40とSACを確立する。SACを確立すると、公開鍵暗号処理部107は、制御部103からサービス用秘密鍵SKを受け取り、また、サーバ装置40との間で確立されたSACを用い、ネットワーク60、通信部101及び制御部103を介して、サーバ装置40から楕円曲線のシステムパラメータ「 $a_2$ 、 $b_2$ 、 $p_2$ 、 $q_2$ 、及び、 $G_2$ 」を受け取る。

#### 【0051】

具体例として、 $a_2 = -3$

$$b_2 = 16461$$

$$p_2 = 20011$$

$$q_2 = 20023$$

$$G_2 = (18892, 5928)$$

とする。公開鍵暗号処理部107は、受け取ったSKとシステムパラメータとから公開鍵

$PK\_B = SK * G_2 \pmod{p_2}$  を算出し、算出した公開鍵  $PK\_B$  を、サーバ装置 40 との間で確立した  $SAC$  を用い、制御部 103、通信部 101 及びネットワーク 60 を介してサーバ装置 40 へ送信する。

#### 【0052】

次に、端末 10 が、サーバ装置 50 に対してサービスへの加入を要求するときの公開鍵暗号処理部 107 について説明する。公開鍵暗号処理部 107 は、制御部 103 から端末 10 自身の秘密鍵である乱数  $R\_0010$  を受け取り、 $RSA$  暗号を用いて、サーバ装置 50 と  $SAC$  を確立する。 $SAC$  を確立すると、公開鍵暗号処理部 107 は、制御部 103 から  $SK$  を受け取り、また、サーバ装置 50 と確立した  $SAC$  を用いて、ネットワーク 60、通信部 101 及び制御部 103 を介して、サーバ装置 50 から楕円曲線のシステムパラメータ「 $a_3$ 、 $b_3$ 、 $p_3$ 、 $q_3$ 、及び、 $G_3$ 」を受け取る。

#### 【0053】

具体例として、 $a_3 = -3$

$b_3 = 16461$

$p_3 = 20011$

$q_3 = 20023$

$G_3 = (8898, 13258)$

とする。公開鍵暗号処理部 107 は、 $SK$  とシステムパラメータとを用いて、公開鍵  $PK\_C = SK * G_3 \pmod{p_3}$  を算出し、算出した公開鍵  $PK\_C$  を、サーバ装置 50 との間で確立した  $SAC$  を用いて、制御部 103、通信部 101 及びネットワーク 60 を介してサーバ装置 50 へ送信する。

#### 【0054】

上記の様に、端末 10 は、サーバ装置 30 に対するサービス加入要求時に生成した 1 個のサービス用秘密鍵  $SK$  と、各サーバ装置から受信したシステムパラメータとを用いて、各サーバ装置に対応する 3 個の公開鍵  $PK\_A$ 、 $PK\_B$ 、 $PK\_C$  を生成する。ここで、各サーバ装置から受信したシステムパラメータの内、ベースポイント  $G_1$ 、 $G_2$ 、 $G_3$  は、それぞれ異なるため、生成される 3 個の公開鍵は互いに異なる。

#### 【0055】

(サービス利用要求)

ここでは、端末 10 が、サーバ装置 30 に対してサービスの利用を要求するときの公開鍵暗号処理部 107 について説明する。公開鍵暗号処理部 107 は、制御部 103 から  $SK$ 、 $Cert\_A$  及び  $PK\_30$  を受け取り、公開鍵暗号のアルゴリズムとして楕円曲線暗号を用いて、サーバ装置 30 と  $SAC$  を確立する。なお、 $SK$  は、端末 10 のサービス用秘密鍵であり、メモリカード 20 のセキュア領域に格納されている。 $Cert\_A$  は、図 12 (a) に示す様に、サーバ装置 30 から端末 10 へ発行された公開鍵証明書であり、端末 10 が、サーバ装置 30 に対して公開している公開鍵  $PK\_A$ 、サーバ装置 30 による署名データなどを含む。なお、 $Cert\_A$  は、メモリカード 20 の公開鍵格納領域 204c 格納されている。 $PK\_30$  は、サーバ装置 30 の公開鍵であり、記憶部 108 に格納されている。 $SAC$  確立処理の詳細は後述する。

#### 【0056】

次に、端末 10 が、サーバ装置 40 に対してサービスの利用を要求するときの公開鍵暗号処理部 107 について説明する。公開鍵暗号処理部 107 は、制御部 103 から  $SK$ 、 $Cert\_B$  及び  $PK\_40$  を受け取り、公開鍵暗号のアルゴリズムとして楕円曲線暗号を用いて、サーバ装置 40 と  $SAC$  を確立する。 $Cert\_B$  は、図 12 (b) に示す様に、サーバ装置 40 から端末 10 へ発行された公開鍵証明書であり、端末 10 がサーバ装置 40 に対して公開している公開鍵  $PK\_B$ 、サーバ装置 40 による署名データなどを含む。 $Cert\_B$  は、メモリカード 20 の公開鍵格納領域 204c に格納されている。 $PK\_40$  は、サーバ装置 40 の公開鍵であり、記憶部 108 に格納されている。

#### 【0057】

次に、端末 10 が、サーバ装置 50 に対してサービスの利用を要求するときの公開鍵暗

号処理部107について説明する。公開鍵暗号処理部107は、制御部103からSK、Cert\_C及びPk\_50を受け取り、公開鍵暗号のアルゴリズムとして楕円曲線暗号を用いて、サーバ装置50とSACを確立する。Cert\_Cは、図12(c)に示す様に、サーバ装置50から端末10へ発行された公開鍵証明書であり、端末10がサーバ装置50に対して公開している公開鍵Pk\_C、サーバ装置50による署名データなどを含む。Cert\_Cは、メモリカード20の公開鍵格納領域204cに格納されている。Pk\_50は、サーバ装置50の公開鍵であり、記憶部108に格納されている。

#### 【0058】

##### (8) 記憶部108

記憶部108は、制御部103から公開鍵Pk\_30、Pk\_40及びPk\_50を受け取り、受け取った各公開鍵を記憶する。Pk\_30は、サーバ装置30の公開鍵であり、Pk\_40は、サーバ装置40の公開鍵であり、Pk\_50は、サーバ装置50の公開鍵である。

#### 【0059】

##### (9) 再生部109

再生部109は、オーディオデコーダ、ビデオデコーダ、バッファ等を備える。図2に示す様に、再生部109は外部の出力装置と接続されており、デコードしたコンテンツを出力装置へ出力する。なお、出力装置は、具体的には、モニタ及びスピーカである。

#### 2. メモリカード20

メモリカード20は、記録媒体にフラッシュメモリを用いたカード型メモリである。図4は、メモリカード20の構成を機能的に示す機能ブロック図である。同図に示す様に、メモリカード20は、入出力部201、メモリ制御部202、認証部203及びメモリ204から構成される。

#### 【0060】

##### (1) 入出力部201

入出力部201は、複数のピン端子を含み、メモリカード20が端末10のメモリカード入出力部104に挿入された状態において、前記複数のピン端子により、端末10のメモリカード入出力部104から受信したデータをメモリ制御部202へ出力し、メモリ制御部202から受け取ったデータをメモリカード入出力部104へ出力する。

#### 【0061】

一例として、入出力部201は、メモリカード20が端末10に挿入されると、メモリ制御部202を介して認証部203が記憶しているメモリカード番号「20」を受け取り、受け取ったメモリカード番号「20」をメモリカード入出力部104へ出力する。その他、入出力部201が送受信するデータは、後述する情報セキュリティシステム1の動作の説明において順次説明する。

#### 【0062】

##### (2) メモリ制御部202

メモリ制御部202は、入出力部201を介して端末10から受け取る指示に従い、メモリ204からデータを読み出し、読み出したデータを入出力部201を介して端末10へ送信する。また、メモリ制御部202は、入出力部201を介して端末10からデータを受信し、受信したデータをメモリ204に格納する。

#### 【0063】

メモリ制御部202は、入出力部201を介して端末10から乱数R\_0を受信し、受信した乱数R\_0を認証部203へ出力する。また、メモリ制御部202は、認証部203から暗号文E2を受け取り、受け取ったE2を入出力部201を介して端末10へ出力する。

##### (3) 認証部203

認証部203は、マイクロプロセッサ、ROM、RAMなどを備える。ROM又はRAMには、認証用プログラムが記憶されており、マイクロプロセッサにより前記認証用プログラムが実行される。なお、ROMには予めメモリカード番号「20」と認証用パスワード



ド「PW\_0」とが記憶されている。メモリカード番号「20」は、メモリカード20を識別するための番号である。PW\_0は、端末10と共有している秘密のデータであって、端末10のメモリカード認証部105との間で行われるチャレンジ-レスポンス型の認証処理に用いられる。

#### 【0064】

認証部203は、入出力部201を介して、端末10から乱数R\_0を受信し、受信した乱数R\_0を暗号鍵として用い、認証用パスワードPW\_0に暗号アルゴリズムEを施して暗号文E2を生成する。認証部203は、生成した暗号文E2を、メモリ制御部202及び入出力部201を介して端末10へ送信する。

なお、ここで用いられる暗号アルゴリズムEの一例は、DESである。

#### 【0065】

##### (4) メモリ204

メモリ204は、具体的にはEEPROMなどから構成される記憶装置であって、セキュア領域204aと、コンテンツ格納領域204bと、公開鍵格納領域204cとを備える。

セキュア領域204aは、内部解析、改竄が物理的及び理論的に不可能な耐タンパー性を有する記憶領域である。セキュア領域204aは、端末10の秘密鍵であるR\_001と、サービス用秘密鍵SKとを内部に格納する。なお、メモリ204全体の記憶容量に対して、セキュア領域204aの記憶容量は微小なサイズである。

#### 【0066】

コンテンツ格納領域204bは、端末10が、サーバ装置30、サーバ装置40及びサーバ装置50から取得したコンテンツを格納する。

公開鍵格納領域204cは、CAから取得する公開鍵証明書Cert\_0010、及び、サーバ装置30から取得する公開鍵証明書Cert\_Aと、サーバ装置40から取得する公開鍵証明書Cert\_Bと、サーバ装置50から取得する公開鍵証明書Cert\_Cとを内部に格納する。

#### 【0067】

##### 3. サーバ装置30

サーバ装置30は、コンテンツ配信業者が有する装置であり、ネットワーク60を介して接続された端末10からサービス加入要求を受け付けると、端末10を登録する。また、サーバ装置30は、登録済みである端末10からサービス利用要求を受け付けると、端末10にコンテンツを提供する。

#### 【0068】

図5は、サーバ装置30の構成を機能的に示す機能ブロック図である。同図に示す様に、サーバ装置30は、通信部301、制御部302、CRL格納部303、Cert管理部304、登録情報管理部305、公開鍵暗号処理部306及びコンテンツ格納部307から構成される。

サーバ装置30は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット等から構成されるコンピュータシステムである。

#### 【0069】

##### (1) 通信部301

通信部301は、Webブラウザを備えるネットワーク接続ユニットであって、ネットワーク60を介して端末10と接続されている。

通信部301は、端末10から情報を受信し、受信した情報を制御部302へ出力する。また、通信部301は、制御部302から情報を受け取り、受け取った情報を端末10へ送信する。

#### 【0070】

通信部301が端末10から受信する情報の具体例は、公開鍵PK\_A、SAC確立に用いる署名データ及び鍵情報などである。通信部301が端末10へ送信する情報の具体例は、公開鍵証明書Cert\_A、SAC確立に用いる署名データ、鍵情報、楕円曲線の

システムパラメータ、コンテンツなどである。

更に、通信部301は、ネットワーク60を介して、CAと接続されており、通信部301は、CAとの間で以下の様に情報の送受信を行う。

【0071】

通信部301は、ネットワーク60を介してCAから常に最新のCRLを受信し、受信した最新のCRLを、制御部302を介してCRL格納部303に格納する。

通信部301は、制御部302を介して公開鍵暗号処理部306から公開鍵「PK\_\_0030」を受け取り、受け取った公開鍵をネットワーク60を介してCAへ送信する。また、通信部301は、ネットワーク60を介してCAから公開鍵「PK\_\_0030」に対応する公開鍵証明書「Cert\_\_0030」を受信し、受信した公開鍵証明書を制御部302へ出力する。

【0072】

通信部301は、ネットワーク60を介してCAから楕円曲線のシステムパラメータを取得し、取得したシステムパラメータを制御部302へ出力する。

(2) 制御部302

制御部302は、マイクロプロセッサ、ROM、RAMなどから構成され、コンピュータプログラムをマイクロプロセッサが実行することにより、制御部302は、サーバ装置30の全体を制御する。

【0073】

(a) 制御部302は、端末10との通信に先立ち、CAから公開鍵証明書の発行を受ける。より具体的には、通信部301は、公開鍵暗号処理部306から出力される公開鍵「PK\_\_0030」と予め内部に記憶している自身のデバイスID「ID\_\_0030」とを、通信部301を介してCAへ送信する。制御部302は、通信部301を介して公開鍵「PK\_\_0030」に対応する公開鍵証明書「Cert\_\_0030」をCAから受信し、受信した公開鍵証明書を、Cert管理部304に出力する。

【0074】

(b) 制御部302は、端末10からサービス加入要求を受け付けると、Cert管理部304から「Cert\_\_0030」を読み出す。更に、制御部302は、端末10とSACを確立する指示を公開鍵暗号処理部306に出力する。端末10との間でSACが確立されると、制御部302は、CAから取得した楕円曲線のシステムパラメータ「 $a_1$ 、 $b_1$ 、 $p_1$ 、 $q_1$ 、及び、 $G_1$ 」を、公開鍵暗号処理部306から受け取るセッション鍵で暗号化したのち、通信部301及びネットワーク60を介して端末10へ送信する。

【0075】

具体的に、サーバ装置30が受信するシステムパラメータは、

$$a_1 = -3$$

$$b_1 = 16461$$

$$p_1 = 20011$$

$$q_1 = 20023$$

$$G_1 = (1, 7553)$$

であるとする。

【0076】

(c) SAC確立処理の一環として、CRL格納部303から最新のCRLを読み、認証相手である端末10が、無効化された装置であるか否かを判断する。

(d) 制御部302は、端末10からCert\_\_Aを含むサービス利用要求を受け取ると、Cert\_\_Aが確かにサーバ装置30自身が端末10へ発行した公開鍵証明書であるか否かを判定する。このとき、制御部302は、登録情報管理部305に管理されている登録情報を参照する。端末10から受信したCert\_\_Aが正しければ、制御部302は、公開鍵暗号処理部306へ、SAC確立処理の指示を出す。

【0077】

(e) 制御部302は、サーバ装置30と端末10とがSACを確立した後、端末10

との間で情報を送受信する際に、公開鍵暗号処理部 306 からセッション鍵を受け取り、受け取ったセッション鍵を暗号鍵又は復号鍵として用い、情報を暗号化して端末 10 へ送信したり、端末 10 から受信する暗号化された情報を復号したりする。具体例として、制御部 302 は、サービス提供時の処理として、端末 10 と SAC を確立した後、公開鍵暗号処理部 306 からセッション鍵を受け取り、コンテンツ格納部 307 からコンテンツを読み出す。制御部 302 は、読み出したコンテンツをセッション鍵で暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツを、通信部 301 を介して端末 10 へ送信する。

#### 【0078】

##### (3) CRL 格納部 303

CRL 格納部 303 は、RAM で構成され、内部に CRL を格納している。CRL は、不正を行った機器や、秘密鍵が暴露された機器など、無効化された機器の ID が登録されたリストである。CRL は、ネットワーク 60 を介して CA からサーバ装置 30 へ送信される。ここで、サーバ装置 30 は、CA から常に最新の CRL を受信し、受信した最新の CRL をそれまで格納していた CRL に替えて、CRL 格納部 303 に格納する。なお、以下では、CRL 格納部 303 は、端末 10 の CRL 格納部 106 と同様に最新の CRL として、図 3 (b) に示す CRL 130 を格納しているものとする。

#### 【0079】

##### (4) Cert 管理部 304

Cert 管理部 304 は、通信部 301 及び制御部 302 を介して CA から公開鍵証明書 Cert\_\_0030 を受け取り、受け取った Cert\_\_0030 を内部に格納する。

##### (5) 登録情報管理部 305

登録情報管理部 305 は、公開鍵暗号処理部 306 により公開鍵証明書が発行された端末の登録情報を管理する。登録情報は、登録された端末の公開鍵や端末に割り振った会員番号、ユーザに関する情報などを含み、登録され端末及びユーザの管理に用いられる。また、登録情報は、制御部 302 が端末 10 から送信された Cert を検証するときに用いられる。

#### 【0080】

##### (6) 公開鍵暗号処理部 306

公開鍵暗号処理部 306 は、マイクロプロセッサ、ROM、RAM、乱数生成器等から構成される。

公開鍵暗号処理部 306 は、端末 10 との通信に先立ち、乱数生成器で乱数 R\_\_0030 を生成し、生成した R\_\_0030 に基づき、公開鍵 PK\_\_0030 を生成する。公開鍵暗号処理部 306 は、生成した公開鍵 PK\_\_0030 を制御部 302、通信部 301 を介して CA へ送信する。

#### 【0081】

##### (端末 10 の登録)

公開鍵暗号処理部 306 は、秘密鍵 Ks\_\_30 を生成し、制御部 302 から楕円曲線のシステムパラメータを受け取る。公開鍵暗号処理部 306 は、秘密鍵 Ks\_\_30 とシステムパラメータとから、 $Kp\_30 = Ks\_30 * G_1 \pmod{p_1}$  を計算し、公開鍵 Kp\_\_30 を生成する。公開鍵暗号処理部 306 は、生成した公開鍵 Kp\_\_30 を、制御部 302 へ出力する。

#### 【0082】

公開鍵暗号処理部 306 は、サービス加入、登録処理において、端末 10 から公開鍵 PK\_\_A を受け取ると、受け取った公開鍵 PK\_\_A に基づき、公開鍵証明書 Cert\_\_A を生成し、生成した Cert\_\_A を制御部 302 へ出力する。

##### (端末 10 へサービス提供)

公開鍵暗号処理部 306 は、制御部 302 から SAC 確立処理の指示を受けると、端末 10 と SAC を確立しセッション鍵を生成する。SAC 確立の詳細については後述する。

#### 【0083】

## (7) コンテンツ格納部 307

コンテンツ格納部 307 は、具体的にはハードディスクドライブユニットであって、内部にコンテンツを格納している。

## 4. サーバ装置 40

サーバ装置 40 は、サーバ装置 30 を有するコンテンツ配信業者とは異なるコンテンツ配信業者が有する装置である。サーバ装置 40 は、ネットワーク 60 を介して接続された端末 10 からサービス加入要求を受け付けると、端末 10 を登録する。また、サーバ装置 40 は、内部にコンテンツを格納しており、登録済みである端末 10 からサービス利用要求を受け付けると、端末 10 にコンテンツを提供する。

## 【0084】

サーバ装置 40 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット等から構成されるコンピュータシステムである。サーバ装置 40 は、図 5 に示したサーバ装置 30 と同様の構成を有するため、サーバ装置 40 の構成は図示していない。以下では、サーバ装置 30 と異なる部分を中心に、サーバ装置 40 について説明する。

(a) サーバ装置 40 は、端末 10 との通信に先立ち、公開鍵  $PK_{0040}$  を生成し、 $PK_{0040}$  を CA に送信し、CA から公開鍵証明書  $Cert_{0040}$  の発行を受ける。図 9 (c) に示す公開鍵証明書 160 は、 $Cert_{0040}$  のデータ構成を示す図である。CA から取得した  $Cert_{0040}$  は、端末 10 と SAC を確立する処理に用いられる。

## 【0085】

(b) サーバ装置 40 は、CA から楕円曲線のシステムパラメータを受信する。ここで、サーバ装置 40 が受信するシステムパラメータの組は、サーバ装置 40 にユニークであるとする。

具体的に、サーバ装置 40 が受信するシステムパラメータは、

$$a_2 = -3$$

$$b_2 = 16461$$

$$p_2 = 20011$$

$$q_2 = 20023$$

$$G_2 = (18892, 5928)$$

であるとする。

## 【0086】

サーバ装置 40 は、秘密鍵  $Ks_{40}$  を生成し、生成した  $Ks_{40}$  と CA から受信したシステムパラメータとから、楕円曲線上の計算により、 $Kp_{40} = Ks_{40} * G_2 \pmod{p_2}$  を算出し、公開鍵  $Kp_{40}$  を生成する。

サーバ装置 40 は、端末 10 と SAC を確立した後、CA から受信したシステムパラメータと、生成した公開鍵  $Kp_{40}$  とを、端末 10 へ送信する。

## 【0087】

(c) サーバ装置 40 は、端末 10 から公開鍵  $PK_B$  を受信し、受信した公開鍵  $PK_B$  に対して、公開鍵証明書  $Cert_B$  を発行する。図 12 (b) に示した公開鍵証明書 220 は、 $Cert_B$  のデータ構成を示す図である。

(d) サーバ装置 40 は、端末 10 から公開鍵証明書  $Cert_B$  を含むサービス利用要求を受信すると、 $Cert_B$  を検証する。 $Cert_B$  の検証に成功すると、サーバ装置 40 は、端末 10 と SAC を確立し、端末 10 へコンテンツを送信する。

## 【0088】

## 5. サーバ装置 50

サーバ装置 50 は、サーバ装置 30 を有するコンテンツ配信業者、及び、サーバ装置 40 を有するコンテンツ配信業者とは異なるコンテンツ配信業者が有する装置である。サーバ装置 50 は、ネットワーク 60 を介して接続された端末 10 からサービス加入要求を受け付けると、端末 10 を登録する。また、サーバ装置 50 は、内部にコンテンツを格納しており、登録済みである端末 10 からサービス利用要求を受け付けると、端末 10 にコン

テンツを提供する。

#### 【0089】

サーバ装置50は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット等から構成されるコンピュータシステムである。サーバ装置50は、図5に示したサーバ装置30と同様の構成を有するため、サーバ装置50の構成は図示していない。以下では、サーバ装置30及びサーバ装置40と異なる部分を中心に、サーバ装置50について説明する。

#### 【0090】

(a) サーバ装置50は、端末10との通信に先立ち、公開鍵PK\_\_0050を生成し、PK\_\_0050をCAに送信し、CAから公開鍵証明書Cert\_\_0050の発行を受ける。図9(d)に示す公開鍵証明書170は、Cert\_\_0050のデータ構成を示す図である。CAから取得したCert\_\_0050は、端末10とSACを確立する処理に用いられる。

#### 【0091】

(b) サーバ装置50は、CAから楕円曲線のシステムパラメータを受信する。ここで、サーバ装置50が受信するシステムパラメータの組は、サーバ装置50にユニークであるとする。

具体的に、サーバ装置50が受信するシステムパラメータは、

$$a_3 = -3$$

$$b_3 = 16461$$

$$p_3 = 20011$$

$$q_3 = 20023$$

$$G_3 = (8898, 13258)$$

であるとする。

#### 【0092】

サーバ装置50は、秘密鍵Ks\_\_50を生成し、生成したKs\_\_50とCAから受信したシステムパラメータとから、楕円曲線上の計算により、 $K_P\_50 = K_S\_50 * G_3 \pmod{p_3}$ を算出し、公開鍵KP\_\_50を生成する。

サーバ装置50は、端末10とSACを確立した後、CAから受信したシステムパラメータと、生成した公開鍵KP\_\_50とを、端末10へ送信する。

#### 【0093】

(c) サーバ装置50は、端末10から公開鍵PK\_\_Cを受信し、受信した公開鍵PK\_\_Cに対して、公開鍵証明書Cert\_\_Cを発行する。図12(c)に示した公開鍵証明書230は、Cert\_\_Cのデータ構成を示す図である。

(d) サーバ装置50は、端末10から公開鍵証明書Cert\_\_Cを含むサービス利用要求を受信すると、Cert\_\_Cを検証する。Cert\_\_Cの検証に成功すると、サーバ装置50は、端末10とSACを確立し、端末10へコンテンツを送信する。

#### 【0094】

##### <動作>

ここでは、フローチャートを用いて、情報セキュリティシステム1の動作について説明する。

##### (1) 全体の動作1 (サービス加入、登録時)

図6及び図15は、情報セキュリティシステム1全体の動作を示すフローチャートである。図6は「サービス加入、登録時」における情報セキュリティシステム1の動作を示し、図15は「サービス利用時」における情報セキュリティシステム1の動作を示す。

#### 【0095】

まず、メモリカード20が端末10のメモリカード入出力部104に挿入されると(ステップS101)、端末10は、メモリカード20を認証する(ステップS102)。端末10は、メモリカード20の認証に失敗すると(ステップS103でNG)、処理を終了する。端末10は、メモリカード20の認証に成功すると(ステップS103でOK)

、CAから公開鍵証明書が発行を受ける（ステップS104）。

【0096】

サーバ装置30は、予め、CAから公開鍵証明書が発行を受ける（ステップS105）。同様に、サーバ装置40は、予め、CAから公開鍵証明書が発行を受ける（ステップS106）。同様に、サーバ装置50は、予め、CAから公開鍵証明書が発行を受ける（ステップS107）。

続いて、端末10及びサーバ装置30は、サービス加入、登録処理を行う（ステップS108）。次に、端末10とサーバ装置40は、サービス加入、登録処理を行う（ステップS109）。次に、端末10とサーバ装置50は、サービス加入、登録処理を行う（ステップS110）。

【0097】

以上が「サービス加入、登録時」における処理である。

以下、図15に続くが、ここでは、説明の便宜上、図7以降のフローチャートを用いて、サービス加入、登録時における処理の詳細について先に説明し、その後、図15について説明する。

（2）メモリカード20の認証処理

ここでは、図7に示すフローチャートを用いてメモリカード20の認証処理について説明する。なお、ここで説明する動作は、図6のステップS102の詳細である。

【0098】

端末10のメモリカード入出力部104に、メモリカード20が挿入されている状態において、端末10のメモリカード認証部105は、乱数R\_\_0を生成し（ステップS201）、生成した乱数R\_\_0を内部に保持すると共に、メモリカード入出力部104を介してメモリカード20へ送信し、メモリカード20は乱数R\_\_0を受信する（ステップS202）。

【0099】

メモリカード20の認証部203は、入出力部201及びメモリ制御部202を介して乱数R\_\_0を受け取ると、R\_\_0を暗号鍵として用い、内部に保持している認証用パスワードPW\_\_0に暗号アルゴリズムEを施して暗号文E2を生成する（ステップS203）。一方、メモリカード認証部105は、ステップS201で生成した乱数R\_\_0を暗号鍵として用い、メモリカード20と共有している認証用パスワードPW\_\_0に暗号アルゴリズムEを施して暗号文E1を生成する（ステップS204）。

【0100】

メモリカード20の認証部203は、ステップS203で生成した暗号文E2を端末10へ送信し、端末10は、暗号文E2を受信する（ステップS205）。端末10のメモリカード認証部105は、メモリカード入出力部104及び制御部103を介して暗号文E2を受け取ると、受け取った暗号文E2と、ステップS204で生成した暗号文E1とを比較する（ステップS206）。

【0101】

暗号文E1と暗号文E2とが一致する場合（ステップS207でYES）、端末10はメモリカード20の認証に成功であり、メモリカード認証部105は、制御部103へ「認証OK」を示す信号を出力する（ステップS208）。次に、端末10は、図6のステップS103に戻り処理を続ける。

暗号文E1と暗号文E2とが一致しない場合（ステップS207でNO）、端末10は、メモリカード20の認証に失敗であり、メモリカード認証部105は、制御部103へ「認証NG」を示す信号を出力する（ステップS209）。次に、端末10は、図6のステップS103に戻り処理を続ける。

【0102】

（3）CAから公開鍵証明書（Cert）の発行を受ける処理

ここでは、図8に示すフローチャートを用いて、端末10、サーバ装置30、サーバ装置40及びサーバ装置50が、CAから公開鍵証明書の発行を受ける処理について説明す

る。なお、ここで説明する動作は、図6のステップS104、ステップS105、ステップS106及びステップS107の詳細である。

#### 【0103】

端末10、サーバ装置30、サーバ装置40及びサーバ装置50の公開鍵暗号処理部は、それぞれ乱数生成器により乱数R\_\_Lを生成し(ステップS301)、更に、生成した乱数R\_\_Lから公開鍵PK\_\_Lを生成する(ステップS302)。ここで、端末10は、L=0010、サーバ装置30は、L=0030、サーバ装置40は、L=0040、サーバ装置50は、L=0050である。なお、乱数R\_\_Lから公開鍵PK\_\_Lを生成するアルゴリズムは限定しない。一例としては、RSA暗号である。

#### 【0104】

端末10、サーバ装置30、サーバ装置40及びサーバ装置50の公開鍵暗号処理部は、生成した公開鍵PK\_\_Lを制御部へ出力する。制御部は、公開鍵PK\_\_Lと、内部に記憶している自身のデバイスIDとを含む情報を、通信部を介してCAに送信し、CAは、公開鍵PK\_\_LとデバイスIDとを含む情報を受信する(ステップS303)。

CAは、ステップS303で受信した情報の送信元(公開鍵証明書の依頼元)について、公開鍵、メールアドレス、ユーザ、ユーザが属する組織などが確かに存在し、且つ、正しいことを検証する(ステップS304)。

#### 【0105】

依頼元が不正な場合(ステップS305でNO)、CAは、処理を終了する。

依頼元が正当な場合(ステップS305でYES)、CAは、受信した公開鍵PK\_\_L及びデバイスIDに署名データSig\_\_LCAを付加し、公開鍵証明書Cert\_\_Lを生成する(ステップS306)。CAは、生成した公開鍵証明書Cert\_\_Lを依頼元の端末10、サーバ装置30、サーバ装置40及びサーバ装置50へ送信し、端末10、サーバ装置30、サーバ装置40及びサーバ装置50は、公開鍵証明書Cert\_\_Lを受信する(ステップS307)。

#### 【0106】

端末10は、受信した公開鍵証明書Cert\_\_0010を、制御部103及びメモリカード入出力部104を介して、メモリカード20の公開鍵格納領域204cに格納する(ステップS308)。ここで、端末10がCAから受信した公開鍵証明書Cert\_\_0010のデータ構成を図9(a)に示す。同図に示す様に、Cert\_\_0010は、ID\_\_0010と、PK\_\_0010と、Sig\_\_0010CAとを含む。なお、ID\_\_0010は、端末10のデバイスIDである。

#### 【0107】

サーバ装置30は、ステップS307で受信した公開鍵証明書Cert\_\_0030を、制御部302を介してCert管理部304に格納する(ステップS308)。図9(b)は、サーバ装置30がCAから受信した公開鍵証明書Cert\_\_0030のデータ構成を示す図である。同図に示す様に、Cert\_\_0030は、ID\_\_0030と、PK\_\_0030と、ID\_\_0030と、Sig\_\_0030CAとを含む。なお、ID\_\_0030は、サーバ装置30のデバイスIDである。

#### 【0108】

サーバ装置40及びサーバ装置50も同様に、それぞれがステップS307で受信した公開鍵証明書Cert\_\_0040及びCert\_\_0050を内部に格納する(ステップS308)。図9(c)は、サーバ装置40がCAから受信した公開鍵証明書Cert\_\_0040のデータ構成を示す図であり、図9(d)は、サーバ装置50がCAから受信した公開鍵証明書Cert\_\_0050のデータ構成を示す図である。

#### 【0109】

CAから公開鍵証明書を取得すると、端末10及びサーバ装置30は、図6のステップS108の処理に続く。サーバ装置40は、ステップS109の処理に続き、サーバ装置50は、ステップS110の処理に続く。

(4) サービス加入、登録処理

ここでは、図10及び図11に示すフローチャートを用いて、端末10とサーバ装置30とによるサービス加入、登録処理（図6のステップS108）、端末10とサーバ装置40とによるサービス加入、登録処理（図6のステップS109）、及び、端末10とサーバ装置50とによるサービス加入、登録処理（図6のステップS110）の動作について説明する。なお、ここでは、サーバ装置30、サーバ装置40及びサーバ装置50を、単に「サーバ装置」と呼称することがある。

#### 【0110】

端末10において、操作入力部102を介してユーザの入力を受け付けることにより、サーバ装置に対するサービス加入要求が発生すると（ステップS401）、端末10とサーバ装置との間でSAC確立の処理を行う（ステップS402）。

サーバ装置は、CAから楕円曲線 $y^2 = x^3 + ax + b$ のシステムパラメータを取得する（ステップS403）。ここで、サーバ装置30がCAから取得するシステムパラメータは「 $a_1$ 、 $b_1$ 、 $p_1$ 、 $q_1$ 、及び、 $G_1$ 」であり、サーバ装置40がCAから取得するシステムパラメータは「 $a_2$ 、 $b_2$ 、 $p_2$ 、 $q_2$ 、及び、 $G_2$ 」であり、サーバ装置50がCAから取得するシステムパラメータは「 $a_3$ 、 $b_3$ 、 $p_3$ 、 $q_3$ 、及び、 $G_3$ 」である。

#### 【0111】

サーバ装置の制御部は、取得したシステムパラメータを、ステップS402のSAC確立処理で端末10と共有したセッション鍵を暗号鍵として用い、暗号化する（ステップS404）。なお、ここで用いる暗号アルゴリズムの一例はDES（Data Encryption Standard）である。サーバ装置の制御部は、暗号化したシステムパラメータを、通信部及びネットワーク60を介して端末10へ送信し、端末10の通信部101は、システムパラメータを受信する（ステップS405）。

#### 【0112】

端末10の制御部103は、ステップS402のSAC確立処理でサーバ装置と共有したセッション鍵を復号鍵として用い、暗号化されたシステムパラメータを復号する（ステップS406）。端末10の公開鍵暗号処理部107は、サービス用秘密鍵SKを既に生成しており、メモ리카ード20のセキュア領域204aにSKが格納されている場合（ステップS407でYES）、ステップS409に進む。端末10の公開鍵暗号処理部107は、サービス用秘密鍵SKを未だ生成しておらず、メモ리카ード20のセキュア領域204aにSKが格納されていない場合（ステップS407でNO）、乱数生成器により、サービス用秘密鍵SKを生成する（ステップS408）。

#### 【0113】

公開鍵暗号処理部107は、サービス用秘密鍵SKとサーバ装置から取得したシステムパラメータとを用いて、次式を計算することにより、公開鍵PK\_\_Nを生成する（ステップS409）。

$$PK\_N = SK * G \pmod{p}, N = A, B, \text{及び}, C$$

なお、サービス用秘密鍵SKは、ステップS408において生成した鍵データ、若しくは、既に生成されてメモ리카ード20のセキュア領域204aに格納されている鍵データである。

#### 【0114】

PK\_\_Aは、サーバ装置30から受信するシステムパラメータに基づき生成された公開鍵であり、PK\_\_Bは、サーバ装置40から受信するシステムパラメータに基づき生成された公開鍵であり、PK\_\_Cは、サーバ装置50から受信するシステムパラメータに基づき生成された公開鍵である。

次に、端末10の制御部103は、セッション鍵を暗号鍵として用い、生成した公開鍵PK\_\_Nを暗号化し（ステップS410）、暗号化したPK\_\_Nを、通信部101及びネットワーク60を介してサーバ装置へ送信し、サーバ装置の通信部は、暗号化された公開鍵PK\_\_Nを受信する（ステップS411）。サーバ装置の制御部は、暗号化された公開鍵PK\_\_Nをセッション鍵を用いて復号する（ステップS412）。

#### 【0115】



続いて、サーバ装置の公開鍵暗号処理部は、端末10から受信した公開鍵 $PK\_N$ に対して公開鍵証明書 $Cert\_N$ を生成する（ステップS413）、次に、公開鍵暗号処理部は、乱数生成器を用いて秘密鍵 $Ks\_M$ を生成し（ $M=30$ 、 $40$ 、及び、 $50$ ）、生成した秘密鍵 $Ks\_M$ から公開鍵 $Kp\_M=Ks\_M * G$ を算出する（ステップS415）。 $G$ は、楕円曲線のベースポイントである。サーバ装置の制御部は、セッション鍵を暗号鍵として用い、公開鍵証明書 $Cert\_N$ 及び公開鍵 $Kp\_M$ を暗号化し、暗号化した $Cert\_N$ 及び $Kp\_M$ を通信部及びネットワーク60を介して端末10へ送信し、端末10の通信部101は、暗号化された $Cert\_N$ 及び $Kp\_M$ を受信する（ステップS417）。

#### 【0116】

端末10の制御部103は、受信した $Cert\_N$ 及び $Kp\_M$ をセッション鍵を用いて復号し（ステップS418）、復号した公開鍵証明書 $Cert\_N$ をメモリカード入出力部104を介して、メモリカード20のセキュア領域204aに格納し（ステップS419）、サーバ装置の公開鍵 $Kp\_M$ を記憶部108に格納する（ステップS420）。

#### 【0117】

一方、サーバ装置の登録情報管理部は、端末10に関する登録情報を生成して管理する（ステップS421）。登録情報は、端末10の公開鍵や端末10に割り振った会員番号などを含む。

ここで、各サーバ装置が生成し、端末10へ発行する公開鍵証明書 $Cert\_N$ について図12を用いて説明する。

#### 【0118】

図12（a）は、サーバ装置30が端末10に発行する $Cert\_A$ のデータ構成を示す図である。同図に示す様に、 $Cert\_A$ は、サービスID「 $SID\_0123A$ 」、会員番号「 $NO\_0001$ 」、公開鍵「 $PK\_A$ 」及び署名データ「 $Sig\_A$ 」から構成される。

サービスID「 $SID\_0123A$ 」は、サーバ装置30が提供するサービスの内、端末10が利用するサービスの種類を示す。会員番号「 $NO\_0001$ 」は、サーバ装置30に登録される複数の端末から、当該端末を識別するために割り振られた番号である。公開鍵「 $PK\_A$ 」は、端末10が、サービス用秘密鍵 $SK$ と、サーバ装置30から受信した楕円曲線のシステムパラメータとから生成した鍵データである。署名データ「 $Sig\_A$ 」は、サーバ装置30が、「 $SID\_0123A$ 」、「 $NO\_0001$ 」及び「 $PK\_A$ 」に対し、署名アルゴリズムを施して生成したデータである。

#### 【0119】

図12（b）は、サーバ装置40が端末10に発行する $Cert\_B$ のデータ構成を示す図である。同図に示す様に、 $Cert\_B$ は、サービスID「 $SID\_0321B$ 」、会員番号「 $NO\_0025$ 」、公開鍵「 $PK\_B$ 」及び署名データ「 $Sig\_B$ 」から構成される。

サービスID「 $SID\_0321B$ 」は、サーバ装置40が提供するサービスの内、端末10が利用するサービスの種類を示す。会員番号「 $NO\_0025$ 」は、サーバ装置40に登録される複数の端末から、当該端末を識別するために割り振られた番号である。公開鍵「 $PK\_B$ 」は、端末10が、サービス用秘密鍵 $SK$ と、サーバ装置40から受信した楕円曲線のシステムパラメータとから生成した鍵データである。署名データ「 $Sig\_B$ 」は、サーバ装置40が、「 $SID\_0321B$ 」、「 $NO\_0025$ 」及び「 $PK\_B$ 」に対し、署名アルゴリズムを施して生成したデータである。

#### 【0120】

図12（c）は、サーバ装置50が端末10に発行する $Cert\_C$ のデータ構成を示す図である。同図に示す様に、 $Cert\_C$ は、サービスID「 $SID\_0132C$ 」、会員番号「 $NO\_3215$ 」、公開鍵「 $PK\_C$ 」及び署名データ「 $Sig\_C$ 」から構成される。

サービスID「SID\_0132C」は、サーバ装置50が提供するサービスの内、端末10が利用するサービスの種類を示す。会員番号「NO\_3215」は、サーバ装置50に登録される複数の端末から、当該端末を識別するために割り振られた番号である。公開鍵「PK\_C」は、端末10が、サービス用秘密鍵SKと、サーバ装置50から受信した楕円曲線のシステムパラメータとから生成した鍵データである。署名データ「Sig\_C」は、サーバ装置50が、「SID\_0132C」、「NO\_3215」及び「PK\_C」に対し、署名アルゴリズムを施して生成したデータである。

#### 【0121】

##### (5) SACの確立1

ここでは、図13及び図14に示すフローチャートを用いて、サービス加入、登録時における端末10と各サーバ装置とにおけるSAC確立の動作について説明する。なお、ここで説明する動作は、図10のステップS402の詳細である。

ここで、Gen()を鍵生成関数とし、Yをシステム固有のパラメータとする。また、鍵生成関数Gen()は、 $Gen(X, Gen(y, Z)) = Gen(y, Gen(X, Z))$ の関係を満たすものとする。なお、鍵生成関数は、任意の公知技術で実現可能なため、詳細については省略する。

#### 【0122】

まず、端末10の制御部103は、メモリカード入出力部104を介してメモリカード20から公開鍵証明書Cert\_0010を読み出す(ステップS501)。端末10の通信部101はネットワーク60を介して、Cert\_0010をサーバ装置へ送信し、サーバ装置の通信部はCert\_0010を受信する(ステップS502)。サーバ装置は、CAの公開鍵PK\_CAを用いて公開鍵証明書Cert\_0010に含まれる署名データSig\_0010\_CAに対して、署名検証アルゴリズムを施して署名検証する(ステップS503)。なお、サーバ装置は、CAの公開鍵PK\_CAを既知であるとする。検証結果が失敗の場合(ステップS504でNO)、サーバ装置は処理を終了する。検証結果が成功の場合(ステップS504でYES)、サーバ装置の制御部は、CRL格納部からCRLを読み出し(ステップS505)、公開鍵証明書Cert\_0010に含まれるID\_0010がCRLに登録されているか否かを判断する。

#### 【0123】

ID\_0010がCRLに登録されていると判断する場合(ステップS506でYES)、サーバ装置は処理を終了する。ID\_0010がCRLに登録されていないと判断する場合(ステップS506でNO)、サーバ装置の制御部は、Cert管理部から公開鍵証明書Cert\_Lを読み出す(ステップS507)。制御部は、通信部及びネットワーク60を介して公開鍵証明書Cert\_Lを端末10へ送信し、端末10の通信部は、Cert\_Lを受信する(ステップS508)。

#### 【0124】

端末10の制御部103は、公開鍵証明書Cert\_Lを受け取ると、CAの公開鍵PK\_CAを用いてCert\_Lに含まれる署名データSig\_L\_CAに対して、署名検証アルゴリズムを施して署名検証する(ステップS509)。なお、端末10は、CAの公開鍵PK\_CAを既知であるとする。検証結果が失敗の場合(ステップS510でNO)、端末10は処理を終了する。検証結果が成功の場合(ステップS510でYES)、制御部103は、CRL格納部106からCRLを読み出し(ステップS511)、公開鍵証明書Cert\_Lに含まれて受け取ったID\_LがCRLに登録されているか否かを判断する。

#### 【0125】

ID\_LがCRLに登録されていると判断する場合(ステップS512でYES)、端末10は処理を終了する。ID\_LがCRLに登録されていないと判断する場合(ステップS512でNO)、端末10は処理を継続する。

ステップS507の処理に続いて、サーバ装置の公開鍵暗号処理部は、乱数Cha\_Bを生成する(ステップS513)。サーバ装置の通信部は、ネットワーク60を介して乱

数  $Cha\_B$  を端末 10 へ送信し、端末 10 の通信部 101 は、乱数  $Cha\_B$  を受信する（ステップ S514）。

【0126】

端末 10 の制御部 103 は、乱数  $Cha\_B$  を受け取ると、メモリカード入出力部 104 を介してメモリカード 20 のセキュア領域 204a から秘密鍵  $R\_0010$  を読み出し、読み出した秘密鍵  $R\_0010$  と先程受け取った乱数  $Cha\_B$  とを公開鍵暗号処理部 107 へ出力する。公開鍵暗号処理部 107 は、乱数  $Cha\_B$  に、秘密鍵  $R\_0010$  を用いて署名生成アルゴリズムを施して署名データ  $Sig\_a$  を生成する（ステップ S515）。通信部 101 は、公開鍵暗号処理部 107 が生成した署名データ  $Sig\_a$  を、ネットワーク 60 を介してサーバ装置へ送信し、サーバ装置の通信部は、署名データ  $Sig\_a$  を受信する（ステップ S516）。

【0127】

サーバ装置の公開鍵暗号処理部は、制御部を介して署名データ  $Sig\_a$  を受け取ると、ステップ S502 で  $Cert\_0010$  に含んで受け取った公開鍵  $PK\_0010$  を用いて署名データ  $Sig\_a$  に署名検証アルゴリズムを施して署名検証する（ステップ S517）。検証結果が失敗の場合（ステップ S518 で NO）、サーバ装置は処理を終了する。検証結果が成功の場合（ステップ S518 で YES）、サーバ装置は処理を継続する。

【0128】

一方、端末 10 は、ステップ S515 の処理に続いて、公開鍵暗号処理部 107 において乱数  $Cha\_A$  を生成する（ステップ S519）。公開鍵暗号処理部 107 は、生成した乱数  $Cha\_A$  を、制御部 103、通信部 101 及びネットワーク 60 を介してサーバ装置へ送信し、サーバ装置の通信部は、乱数  $Cha\_A$  を受信する（ステップ S520）。

【0129】

サーバ装置の制御部は、受信した乱数  $Cha\_A$  を公開鍵暗号処理部へ出力し、公開鍵暗号処理部は、受け取った乱数  $Cha\_A$  に、内部に保持している秘密鍵  $R\_L$  を用い、署名アルゴリズムを施して署名データ  $Sig\_b$  を生成する（ステップ S521）。サーバ装置は、生成した署名データ  $Sig\_b$  を制御部、通信部及びネットワーク 60 を介して端末 10 へ送信し、端末 10 の通信部 101 は、署名データ  $Sig\_b$  を受信する（ステップ S522）。

【0130】

端末 10 の公開鍵暗号処理部 107 は制御部 103 を介して、署名データ  $Sig\_b$  を受け取ると、ステップ S508 で  $Cert\_L$  に含んで受け取った公開鍵  $PK\_L$  を用いて署名データ  $Sig\_b$  に署名検証アルゴリズムを施して署名検証する（ステップ S523）。検証結果が失敗の場合（ステップ S524 で NO）、端末 10 は処理を終了する。検証結果が成功の場合（ステップ S524 で YES）、端末 10 の公開鍵暗号処理部 107 は、乱数「a」を生成し（ステップ S525）、生成した乱数「a」を用いて  $Key\_A = Gen(A, Y)$  を生成する（ステップ S526）。端末 10 の通信部 101 は、公開鍵暗号処理部 107 により生成された  $Key\_A$  をネットワーク 60 を介してサーバ装置へ送信し、サーバ装置の通信部は、 $Key\_A$  を受信する（ステップ S527）。

【0131】

サーバ装置の公開鍵暗号処理部は、 $Key\_A$  を受け取ると、乱数「b」を生成し（ステップ S528）、生成した乱数「b」を用いて  $Key\_B = Gen(B, Y)$  を生成する（ステップ S529）。サーバ装置の通信部は、公開鍵暗号処理部により生成された  $Key\_B$  をネットワーク 60 を介して端末 10 へ送信し、端末 10 の通信部は、 $Key\_B$  を受信する（ステップ S530）。また、サーバ装置の公開鍵暗号処理部は、ステップ S528 で生成した乱数「b」と、ステップ S527 で受け取った  $Key\_A$  とを用いて、 $Key\_AB = Gen(B, Key\_A) = Gen(B, Gen(A, Y))$  を生成し（ステップ S531）、生成した  $Key\_AB$  をセッション鍵として制御部へ出力する（

ステップS532)。その後サーバ装置は、図10のステップS403に戻って処理を続ける。

#### 【0132】

一方、端末10の公開鍵暗号処理部107は、ステップS530でKey\_\_Bを受け取ると、Key\_\_BとステップS525で生成した乱数「a」とから $Key\_AB = Gen(a, Key\_B) = Gen(a, Gen(B, y))$ を生成し(ステップS533)、生成したKey\_\_ABをセッション鍵として制御部103へ出力する(ステップS534)。その後端末10は、図10のステップS406に戻って処理を続ける。

#### 【0133】

##### (6) 全体の動作2 (サービス利用時)

ここでは、図1のフローチャートから続く情報セキュリティシステム1全体の動作について図15に示すフローチャートを用いて説明する。なお、図15に示す動作は、情報セキュリティシステム1全体の動作の内、「サービス利用時」における動作である。なお、ここでは、サーバ装置30、サーバ装置40及びサーバ装置50を、単に「サーバ装置」と呼称することがある。

#### 【0134】

端末10において、操作入力部102を介してユーザの入力を受け付けることにより、サーバ装置に対するサービス利用要求が発生すると(ステップS601)、制御部103は、メモリカード入出力部104を介してメモリカード20のセキュア領域204aから、ユーザが指定したサーバ装置により発行された公開鍵証明書Cert\_\_N(N=A、B、又はC)を読み出す(ステップS602)。制御部103は、読み出した公開鍵証明書Cert\_\_Nを、通信部101及びネットワーク60を介して指定のサーバ装置へ送信し、サーバ装置の通信部は公開鍵証明書Cert\_\_Nを受信する(ステップS603)。

#### 【0135】

サーバ装置の制御部は、公開鍵証明書Cert\_\_Nを受け取ると、以下に示す様に受け取ったCert\_\_Nが正しいか否か検証する(ステップS604)。制御部は、登録情報管理部から端末10に対応する登録情報を読み出し、受け取ったCert\_\_Nに含まれるサービスID、会員番号及び端末10の公開鍵が登録されている情報と一致するか否か判断する。更に、制御部は、Cert\_\_Nに含まれる署名データSig\_\_Nを公開鍵暗号処理部へ出力する。Sig\_\_Nを受け取った公開鍵暗号処理部は、受け取った署名データSig\_\_Nに署名検証アルゴリズムを施してSig\_\_Nを検証し、検証結果を制御部へ出力する。

#### 【0136】

Cert\_\_Nの検証に失敗した場合(ステップS605でNG)、サーバ装置は処理を終了する。Cert\_\_Nの検証に成功した場合(ステップS605でOK)、サーバ装置と端末10とは、SACを確立する処理を行う(ステップS606)。

端末10とSACを確立すると、サーバ装置の制御部は、コンテンツ格納部からコンテンツを読み出し(ステップS607)、ステップS606において端末10と共有したセッション鍵を暗号鍵として用い、読み出したコンテンツを暗号化する(ステップS608)。ここで用いる暗号アルゴリズムの一例はDESである。サーバ装置の通信部は、ネットワーク60を介して暗号化コンテンツを端末10へ送信し、端末10の通信部101は、暗号化コンテンツを受信する(ステップS609)。

#### 【0137】

端末10の制御部103は、暗号化コンテンツを受け取ると、ステップS606においてサーバ装置と共有したセッション鍵を復号鍵として用い、受け取った暗号化コンテンツを復号する(ステップS610)。制御部103は、メモリカード入出力部104を介して、復号したコンテンツをメモリカード20のコンテンツ格納領域204bに格納する(ステップS611)。

#### 【0138】

##### (7) SACの確立2

ここでは、図16、図17及び図18に示すフローチャートを用いて、サービス利用時における端末10と各サーバ装置とにおけるSAC確立処理の動作について説明する。なお、ここで説明する動作は、図15のステップS606の詳細である。

ここで、Gen()を鍵生成関数とし、Yをシステム固有のパラメータとする。また、鍵生成関数Gen()は、 $\text{Gen}(X, \text{Gen}(y, Z)) = \text{Gen}(y, \text{Gen}(X, Z))$ の関係を満たすものとする。

#### 【0139】

まず、端末10の制御部103は、メモリカード入出力部104を介してメモリカード20から公開鍵証明書Cert\_\_0010を読み出す(ステップS701)。端末10の通信部101はネットワーク60を介して、Cert\_\_0010をサーバ装置へ送信し、サーバ装置の通信部はCert\_\_0010を受信する(ステップS702)。サーバ装置の公開鍵暗号処理部は、CAの公開鍵PK\_\_CAを用いて公開鍵証明書Cert\_\_0010に含まれる署名データSig\_\_0010CAに対して、署名検証アルゴリズムを施して署名検証する(ステップS703)。検証結果が失敗の場合(ステップS704でNO)、サーバ装置は処理を終了する。検証結果が成功の場合(ステップS704でYES)、サーバ装置の制御部は、CRL格納部からCRLを読み出し(ステップS705)、公開鍵証明書Cert\_\_0010に含まれるID\_\_0010がCRLに登録されているか否かを判断する。

#### 【0140】

ID\_\_0010がCRLに登録されていると判断する場合(ステップS706でYES)、サーバ装置は処理を終了する。ID\_\_0010がCRLに登録されていないと判断する場合(ステップS706でNO)、サーバ装置の制御部は、Cert管理部から公開鍵証明書Cert\_\_Lを読み出す(ステップS707)。制御部は、通信部及びネットワーク60を介して公開鍵証明書Cert\_\_Lを端末10へ送信し、端末10の通信部は、Cert\_\_Lを受信する(ステップS708)。

#### 【0141】

端末10の制御部103は、公開鍵証明書Cert\_\_Lを受け取ると、CAの公開鍵PK\_\_CAを用いてCert\_\_Lに含まれる署名データSig\_\_LCAに対して、署名検証アルゴリズムを施して署名検証する(ステップS709)。検証結果が失敗の場合(ステップS710でNO)、端末10は処理を終了する。検証結果が成功の場合(ステップS710でYES)、制御部103は、CRL格納部106からCRLを読み出し(ステップS711)、公開鍵証明書Cert\_\_Lに含まれて受け取ったID\_\_LがCRLに登録されているか否かを判断する。

#### 【0142】

ID\_\_LがCRLに登録されていると判断する場合(ステップS712でYES)、端末10は処理を終了する。ID\_\_LがCRLに登録されていないと判断する場合(ステップS712でNO)、端末10は処理を継続する。

ステップS707の処理に続いて、サーバ装置の公開鍵暗号処理部は、乱数Cha\_\_Dを生成する(ステップS713)。サーバ装置の通信部は、ネットワーク60を介して乱数Cha\_\_Dを端末10へ送信し、端末10の通信部101は、乱数Cha\_\_Dを受信する(ステップS714)。

#### 【0143】

端末10の公開鍵暗号処理部107は、Cha\_\_Dを受け取ると、 $R1 = (rx, ry) = \text{Cha\_D} * G$ を計算し(ステップS715)、

$$S \times \text{Cha\_D} = m + rx \times SK \pmod{q}$$

から、Sを計算する(ステップS716)。ここで、qは、楕円曲線Eの位数であり、mは、端末10がサーバ装置へ送信するメッセージであり、SKは、メモリカード入出力部104を介してメモリカード20のセキュア領域204aから読み出した端末10のサービス用秘密鍵である。

## 【0144】

端末10は、得られたR1とSとから署名データ  $Sig\_d = (R1, S)$  を生成し（ステップS717）、生成した署名データ  $Sig\_d$  とメッセージmと共にサーバ装置へ送信し、サーバ装置は署名データ  $Sig\_d$  とメッセージmとを受信する（ステップS718）。

サーバ装置の公開鍵暗号処理部は、

$$m * G + r_x * PK\_N$$

を計算し、更に、

$$S * R1$$

を計算する（ステップS719）。

## 【0145】

サーバ装置の公開鍵暗号処理部は、 $S * R1 = m * G + r_x * PK\_N$  が成立するかどうか判定することにより、送信者である端末10の身元を確認する（ステップS720）。これは、

$$\begin{aligned} S * R1 &= \{ (m + r_x \times SK) / Cha\_D \} \times Cha\_D * G \\ &= (m + r_x \times SK) * G \\ &= m * G + (r_x \times SK) * G \\ &= m * G + r_x * PK\_N \end{aligned}$$

となることから明らかである。

## 【0146】

$S * R1 \neq m * G + r_x * PK\_N$  の場合（ステップS720でNO）、サーバ装置は処理を終了する。 $S * R1 = m * G + r_x * PK\_N$  の場合（ステップS720でYES）、サーバ装置は、処理を続ける。

一方で、端末10は、ステップS718において  $Sig\_d$  及びmをサーバ装置へ送信した後、公開鍵暗号処理部107は、乱数  $Cha\_E$  を生成し（ステップS721）、生成した乱数  $Cha\_E$  を制御部103、通信部101ネットワーク60を介してサーバ装置へ送信し、サーバ装置の通信部は  $Cha\_E$  を受信する（ステップS722）。

## 【0147】

サーバ装置の公開鍵暗号処理部は、制御部を介して乱数  $Cha\_E$  を受け取ると、

$$R2 = (r_x, r_y) = Cha\_E * G$$

を計算し（ステップS723）、

$$S' \times Cha\_E = m' + r_x \times Ks\_M \pmod{q}$$

から、 $S'$  を計算する（ステップS724）。ここで、 $m'$  は、サーバ装置が端末10へ送信するメッセージであり、 $Ks\_M$  ( $M=30, 40$ 、又は50) は、サーバ装置の秘密鍵である。より具体的に、 $Ks\_30$  は、サーバ装置30の秘密鍵であり、 $Ks\_40$  は、サーバ装置40の秘密鍵であり、 $Ks\_50$  は、サーバ装置50の秘密鍵である。

## 【0148】

サーバ装置は、得られたR2と  $S'$  とから、署名データ  $Sig\_e = (R2, S')$  を生成し（ステップS725）、生成した署名データ  $Sig\_e$  をメッセージ  $m'$  と共に端末10へ送信し、端末10は署名データ  $Sig\_e$  とメッセージ  $m'$  とを受信する（ステップS726）。

端末10の公開鍵暗号処理部107は、

$$m' * G + r_x * Kp\_M$$

を計算する（ステップS731）。ここで、 $Kp\_M$  ( $M=30, 40$ 、又は50) は、 $Kp\_M = Ks\_M * G$  を計算することにより生成された各サーバ装置の公開鍵である。より具体的に、 $Kp\_30$  は、サーバ装置30の公開鍵であり、 $Ks\_30$  に対応している。 $Kp\_40$  は、サーバ装置40の公開鍵であり、秘密鍵  $Ks\_40$  に対応している。 $Kp\_50$  は、サーバ装置50の公開鍵であり、秘密鍵  $Ks\_50$  に対応している。

## 【0149】

公開鍵暗号処理部107は、更に、

$S' * R2$

を計算する(ステップS731)。

公開鍵暗号処理部107は、 $S' * R2 = m' * G + r_x * Kp\_M$ が成立するかどうか判定することにより、送信者である端末10の身元を確認する(ステップS732)。これは、

$$\begin{aligned} S' * R2 &= \{ (m' + r_x \times Ks\_M) / Cha\_E \} \times Cha\_E * G \\ &= (m' + r_x \times Ks\_M) * G \\ &= m' * G + (r_x \times Ks\_M) * G \\ &= m' * G + r_x * Kp\_M \end{aligned}$$

となることから明らかである。

#### 【0150】

$S' * R2 \neq m' * G + r_x * Kp\_M$ の場合(ステップS732でNO)、端末10は処理を終了する。 $S' * R2 = m' * G + r_x * Kp\_M$ の場合(ステップS732でYES)、公開鍵暗号処理部107は、乱数「d」を生成し(ステップS733)、生成した乱数「d」を用いて $Key\_D = Gen(D, Y)$ を生成する(ステップS734)。端末10の通信部101は、公開鍵暗号処理部107により生成された $Key\_D$ をネットワーク60を介してサーバ装置へ送信し、サーバ装置の通信部は、 $Key\_D$ を受信する(ステップS735)。

#### 【0151】

サーバ装置の公開鍵暗号処理部は、 $Key\_D$ を受け取ると、乱数「e」を生成し(ステップS736)、生成した乱数「e」を用いて $Key\_E = Gen(E, Y)$ を生成する(ステップS737)。サーバ装置の通信部は、公開鍵暗号処理部により生成された $Key\_E$ をネットワーク60を介して端末10へ送信し、端末10の通信部は、 $Key\_E$ を受信する(ステップS738)。また、サーバ装置の公開鍵暗号処理部は、ステップS735で生成した乱数「e」と、ステップS735で受け取った $Key\_D$ とを用いて、 $Key\_DE = Gen(e, Key\_D) = Gen(e, Gen(D, Y))$ を生成し(ステップS741)、生成した $Key\_DE$ をセッション鍵として制御部へ出力する(ステップS742)。その後サーバ装置は、図15のステップS607に戻って処理を続ける。

#### 【0152】

一方、端末10の公開鍵暗号処理部107は、ステップS738で $Key\_E$ を受け取ると、 $Key\_E$ とステップS733で生成した乱数「d」とから $Key\_DE = Gen(d, Key\_E) = Gen(d, Gen(E, Y))$ を生成し(ステップS739)、生成した $Key\_DE$ をセッション鍵として制御部103へ出力する(ステップS740)。その後端末10は、図15のステップS610に戻って処理を続ける。

#### 【0153】

(7) 楕円曲線のシステムパラメータ生成処理の動作

情報セキュリティシステム1において、認証局(CA)は、各機器に公開鍵証明書を発行する機能、及び、暗号に適したシステムパラメータを生成し、生成したシステムパラメータを各サーバ装置へ通知する機能を有する。ここで、システムパラメータは、楕円曲線 $E: y^2 = x^3 + ax + b$ を構成するa、b、素数p、pの位数q、及び、楕円曲線E上のベースポイントGを指す。特に、当該システムにおいて、CAは、サーバ装置毎に固有のシステムパラメータを生成する。

#### 【0154】

ここでは、図19に示すフローチャートを用いて、CAによる楕円曲線のシステムパラメータ生成処理の動作について説明する。

CAが有する楕円曲線管理装置は、乱数を生成し(ステップS801)、生成した乱数を用いて楕円曲線を決定するa、b、素数p及び元Gを生成し、(ステップS802)、生成したパラメータを用いて、楕円曲線の位数を計算する(ステップS803)。

#### 【0155】

次に、計算された位数を用いて、以下に示す安全な楕円曲線の条件を満たすか否かを判定することにより、楕円曲線の安全性を判定する。

現存するすべての解読法に対して安全な楕円曲線の条件は、有限体  $GF(p)$  上の楕円曲線の場合、

(条件1) 楕円曲線の位数が  $p-1$ 、 $p$  及び  $p+1$  のいずれでもないこと、及び

(条件2) この楕円曲線の位数が大きい素因数をもつことである。

#### 【0156】

「暗号・ゼロ知識証明、数論」(155ページ～156ページ、情報処理学会監修、岡本龍明・太田和夫共編、共立出版、1995年)によると、これらの条件を満たす場合に、解読するために必要な計算時間は、前記位数の最大素因数に関する指数関数時間である。

(条件1) 及び (条件2) を満たさない場合 (ステップ S804 で NG)、ステップ S801 に戻り、乱数の生成と、楕円曲線のシステムパラメータの生成と、楕円曲線の位数の計算と、条件判定とを繰り返す。

#### 【0157】

(条件1) 及び (条件2) を満たす場合 (ステップ S804 で OK)、楕円曲線管理装置は、生成されたシステムパラメータを、既に生成され、記憶されているシステムパラメータと比較する (ステップ S805)。生成されたシステムパラメータの組み合わせが、記憶されているシステムパラメータの組み合わせの何れかと一致する場合 (ステップ S806 で YES)、生成したシステムパラメータを破棄し (ステップ S807)、ステップ S801 に戻り処理を続ける。

#### 【0158】

生成されたシステムパラメータの組み合わせが、記憶されているシステムパラメータの組み合わせの何れとも一致しない場合 (ステップ S806 で NO)、生成されたシステムパラメータの組み合わせを記憶すると共に、サーバ装置 30、サーバ装置 40、又はサーバ装置 50 へ送信する (ステップ S808)。

なお、CA が有する楕円曲線管理装置は、サーバ装置 30、サーバ装置 40、及び、サーバ装置 50 から要求を受ける毎に、上記の処理を行うものとする。

#### 【0159】

これにより、サーバ装置 30、サーバ装置 40、及びサーバ装置 50 は、他のサーバ装置と異なるユニークな楕円曲線のシステムパラメータの組み合わせを取得する。

#### <まとめ>

以上説明したように、本発明は、SAC で利用する公開鍵暗号を、一例として楕円曲線暗号であると想定する。楕円曲線暗号では、秘密鍵を生成してから公開鍵を算出するが、公開鍵の算出には、秘密鍵とシステムパラメータとを利用するため、秘密鍵が共通であっても、システムパラメータが異なれば、異なる公開鍵が算出される。

#### 【0160】

そこで、本発明は、コンテンツ配信サービスを提供するサーバ装置が、自身のサービス用のシステムパラメータを、サービス利用者である端末へ送信する。このとき、コンテンツ配信サービスを提供するサーバ装置が複数存在する場合、端末は、複数のサーバ装置から、それぞれ異なるシステムパラメータを取得するものとする。

端末は、既に保持している秘密鍵と受信したパラメータとから公開鍵を算出し、算出した公開鍵をサーバ装置へ返信する。公開鍵を受信したサーバ装置は、公開鍵に対して署名を付与した公開鍵証明書を作成して、端末へ返送する。

#### 【0161】

#### <その他の変形例>

以上、本発明を上記実施の形態に基づき説明してきたが、本発明は上記実施の形態に限定されないのは勿論であり、以下の様な場合も本発明に含まれる。

(1) 上記実施の形態では、端末 10 が各サーバ装置から取得する楕円曲線のシステムパラメータ「 $a$ 、 $b$ 、 $p$ 、 $q$ 、及び、 $G$ 」の内、ベースポイント  $G$  がサーバ装置毎に異なる



る構成を有しているが、本発明は、この構成に限定されないのは勿論である。端末10が各サーバ装置から取得するシステムパラメータ「a、b、p、q、及び、G」の内、少なくとも、素数p又はベースポイントGの何れかが、サーバ装置毎に異なっていればよい。勿論、システムパラメータの各値が、サーバ装置毎に全て異なっている場合も本発明に含まれる。本発明において、端末10が取得する楕円曲線のシステムパラメータの組み合わせがサーバ装置毎に異なるのは、サーバ装置毎に異なる公開鍵を生成することが目的であり、システムパラメータ自体が異なることは目的ではない。

#### 【0162】

(2) 上記実施の形態では、端末10が秘密鍵SKとパラメータとから公開鍵P\_A、PK\_B、及び、PK\_Cを生成する構成を有しているが、公開鍵は必ずしも端末10で生成される必要はなく、以下のような場合も本発明に含まれる。

(a) サーバ装置が公開鍵を生成する

まず、端末と各サーバ装置との間でSACを確立する。

#### 【0163】

端末10は、サービス用秘密鍵SKを生成し、生成したサービス用秘密鍵SKを、SACを介して安全かつ確実に各サーバ装置へ送信する。

各サーバ装置は、端末10のサービス用秘密鍵SKとCAから取得した楕円曲線のシステムパラメータとから、秘密鍵SKに対応する公開鍵を生成する。各サーバ装置は、生成した公開鍵に自身の署名を付加した公開鍵証明書を生成し、生成した公開鍵証明書を端末10へ返信する。

#### 【0164】

(b) 認証局(CA)が公開鍵を生成する

まず、端末10とCAとの間でSACを確立する。

CAは、異なる3組のシステムパラメータを生成する。端末10は、サービス用秘密鍵SKを生成し、生成したサービス用秘密鍵SKをSACを介して安全かつ確実にCAへ送信する。

#### 【0165】

CAは、端末10から秘密鍵SKを受信すると、1個の秘密鍵SKと3組のシステムパラメータとから、異なる3個の公開鍵を生成する。CAは、生成した3個の公開鍵を端末へ送信する。

端末10は、3個の公開鍵を受信すると、それぞれサーバ装置30、サーバ装置40及びサーバ装置50へ送信する。各サーバ装置は、端末10から公開鍵を受信すると、受信した公開鍵に署名を付加して公開鍵証明書を生成し、生成した公開鍵証明書を端末10へ返信する。

#### 【0166】

(3) SAC確立時の署名データ生成及び署名データ検証に用いる公開鍵暗号は、楕円曲線暗号に限定されない。公開鍵暗号としてRSA暗号を用いる構成も本発明に含まれる。ここでは、RSA暗号を用いた実施形態について以下に述べる。

(RSA暗号の基礎的事項)

公開鍵: N、e

秘密鍵: P、Q、d

$$N = P \times Q, (e, (P-1)(Q-1)) = 1$$

$$ed \equiv 1 \pmod{(P-1)(Q-1)}$$

暗号化:  $C = E(M) = M^e \pmod N$

復号:  $M = D(C) = C^d \pmod N$

(動作)

端末10が、サーバ装置30、サーバ装置40及びサーバ装置50から公開鍵証明書の発行を受ける処理の動作について以下に述べる。

#### 【0167】

(ステップ1) 端末10は、任意の相異なる二つの大きな素数P<sub>1</sub>、Q<sub>1</sub>を選ぶ。また、

端末10は、乱数生成器などにより、秘密鍵  $d$  を生成する。

(ステップ2) 端末10は、 $N_1 = P_1 \times Q_1$  を計算する。また、端末10は、 $e_1 d \equiv 1 \pmod{(P_1 - 1)(Q_1 - 1)}$  から、 $e_1$  を計算する。

(ステップ3) 端末10は、公開鍵 ( $N_1$ 、 $e_1$ ) を、サーバ装置30へ送信し、サーバ装置30から公開鍵証明書を受信し、記憶する。

【0168】

(ステップ4) 端末10は、 $P_1$  及び  $Q_1$  を削除し、秘密鍵  $d$  をセキュアな記憶領域に記憶する。

(ステップ5) 端末10は、 $P_1$ 、 $Q_1$  とは異なる大きな素数  $P_2$  及び  $Q_2$  を選ぶ。

(ステップ6) 端末10は、 $N_2 = P_2 \times Q_2$  を計算する。また、端末10は、 $e_2 d \equiv 1 \pmod{(P_2 - 1)(Q_2 - 1)}$  から、 $e_2$  を計算する。

【0169】

(ステップ7) 端末10は、公開鍵 ( $N_2$ 、 $e_2$ ) を、サーバ装置40へ送信し、サーバ装置40から公開鍵証明書を受信し、記憶する。

(ステップ8) 端末10は、 $P_2$  及び  $Q_2$  を削除する。

(ステップ9) 端末10は、 $P_1$ 、 $Q_1$ 、 $P_2$ 、 $Q_2$  とは異なる大きな素数  $P_3$  及び  $Q_3$  を選ぶ。

【0170】

(ステップ10) 端末10は、 $N_3 = P_3 \times Q_3$  を計算する。また、端末10は、 $e_3 d \equiv 1 \pmod{(P_3 - 1)(Q_3 - 1)}$  から、 $e_3$  を計算する。

(ステップ11) 端末10は、公開鍵 ( $N_3$ 、 $e_3$ ) を、サーバ装置50へ送信し、サーバ装置50から公開鍵証明書を受信し、記憶する。

(ステップ12) 端末10は、 $P_3$  及び  $Q_3$  を削除する。

【0171】

この様に、端末10は、楕円曲線のシステムパラメータに替えて、大きな素数の組 ( $P$ 、 $Q$ ) を複数個生成するか、又は、取得し、1個の秘密鍵  $d$  と複数個の素数の組 ( $P$ 、 $Q$ ) とから、RSA暗号のアルゴリズムに従い、複数個の公開鍵 ( $N$ 、 $e$ ) を生成することができる。即ち、端末10は、楕円曲線暗号のみならず、RSA暗号を用いても、1個の秘密鍵から複数個の公開鍵を生成し、生成した複数個の公開鍵を用いて、複数のサーバ装置とSACを確立し、コンテンツの送受信を行うことができる。

【0172】

(4) 上記のRSA暗号を用いた変形例では、端末10が複数個の公開鍵を生成するのではなく、各サーバ装置が公開鍵を生成するように構成されてもよい。

(5) 端末10及び各サーバ装置は、CRLをネットワーク60を介してCAより受信する構成を有しているが、CRLの取得方法はこれに限定されない。放送で受信してもよいし、DVD等の記録媒体に格納して配布されてもよい。

【0173】

(6) メモリカードに秘密鍵、公開鍵、コンテンツを格納しなくても端末内部の記憶領域に格納してもよい。このとき、少なくとも秘密鍵はセキュアな記憶領域に格納されるべきである。

(7) 上記実施の形態では、端末10が、秘密鍵及び公開鍵の生成処理、SAC確立処理の機能を担っているが、本発明は、端末10がこれらの処理を行うことは必須ではなく、ネットワークに接続された端末に挿入されたICチップを備えるメモリカード(以下、「ICメモリカード」と呼称する)が、秘密鍵及び公開鍵の生成処理、SAC確立処理等を行う場合も本発明に含まれる。

【0174】

以下では、ICメモリカードを用いた実施形態について説明する。

ICメモリカードは、端末に挿入されており、端末を介してサーバ装置30、サーバ装置40及びサーバ装置50、並びに、CAと通信可能であるとする。

ICメモリカードは、ICチップ、ROM、RAMなどから構成される制御部と、記憶

領域とから構成される。なお、記憶領域の一部は外部から解読及び改竄が不可能なセキュア領域であるとする。

【0175】

ICメモリカードは、予め、端末を介してCAと通信を行い、CAから、ICメモリカードのデバイスIDとICメモリカードの公開鍵とCAによる署名データとを含む公開鍵証明書の発行を受け、受信した公開鍵証明書を記憶領域に格納している。

更に、ICメモリカードは、サーバ装置30が公開している公開鍵、サーバ40が公開している公開鍵、及び、サーバ装置50が公開している公開鍵を記憶領域に格納している。

【0176】

(サービス加入要求)

ここでは、ICメモリカードが、サーバ装置30に対してサービスへの加入を要求するときの制御部の処理について説明する。

制御部は、公開鍵暗号のアルゴリズムとしてRSA暗号を用い、サーバ装置30とSACを確立する。SAC確立の詳細は、上記実施の形態におけるSAC確立処理と同様であって、上記実施の形態において、端末10が行っていた処理を、ICメモリカードが行う。

【0177】

制御部は、サーバ装置30との間で確立されたSACを用い、端末を介してサーバ装置30から、楕円曲線のシステムパラメータ「 $a_1$ 、 $b_1$ 、 $p_1$ 、 $q_1$ 、及び、 $G_1$ 」を受け取る。

制御部は、サービス用秘密鍵を生成し、生成したサービス用秘密鍵とシステムパラメータとを用いて、公開鍵を算出する。制御部は、生成したサービス用秘密鍵をセキュア領域に書き込み、算出した公開鍵を、サーバ装置30との間で確立されたSACを用い、端末を介してサーバ装置30へ送信する。その後、制御部は、端末を介してサーバ装置30から公開鍵証明書を受け取り、受け取った公開鍵証明書を記憶領域に書き込む。

【0178】

次に、ICメモリカードが、サーバ装置40に対してサービスへの加入を要求するときの制御部の処理について説明する。

制御部は、サーバ装置40とSACを確立し、確立されたSACを用い、端末を介してサーバ装置40から、楕円曲線のシステムパラメータ「 $a_2$ 、 $b_2$ 、 $p_2$ 、 $q_2$ 、及び、 $G_2$ 」を受け取る。

【0179】

制御部は、セキュア領域からサービス用秘密鍵を読み出し、読み出したサービス用秘密鍵とシステムパラメータとを用いて、公開鍵を算出する。制御部は、算出した公開鍵を、サーバ装置40との間で確立されたSACを用い、端末を介してサーバ装置40へ送信する。その後、制御部は、端末を介してサーバ装置40から公開鍵証明書を受け取り、受け取った公開鍵証明書を記憶領域に書き込む。

【0180】

次に、ICメモリカードが、サーバ装置50に対してサービスへの加入を要求するときの制御部の処理について説明する。

制御部は、サーバ装置50とSACを確立し、確立されたSACを用い、端末を介してサーバ装置50から、楕円曲線のシステムパラメータ「 $a_3$ 、 $b_3$ 、 $p_3$ 、 $q_3$ 、及び、 $G_3$ 」を受け取る。

【0181】

制御部は、セキュア領域からサービス用秘密鍵を読み出し、読み出したサービス用秘密鍵とシステムパラメータとを用いて、公開鍵を算出する。制御部は、算出した公開鍵を、サーバ装置50との間で確立されたSACを用い、端末を介してサーバ装置50へ送信する。その後、制御部は、端末を介してサーバ装置50から公開鍵証明書を受け取り、受け取った公開鍵証明書を記憶領域に書き込む。

**【0182】**

この様に、ICメモリカードはサーバ装置30に対するサービス加入要求時に生成した1個のサービス用秘密鍵と、各サーバ装置から受信したシステムパラメータとを用いて、各サーバ装置に対応する3個の異なる公開鍵を生成することが出来る。

**(サービス利用要求)**

ここでは、ICメモリカードが、サーバ装置30に対してサービスの利用を要求するときの制御部の処理について説明する。

**【0183】**

制御部は、記憶領域からサービス用秘密鍵、公開鍵証明書（サーバ装置30から発行されたもの）、及び、サーバ装置30の公開鍵を読み出し、読み出したこれらの鍵情報を用いてサーバ装置30とSACを確立する。SAC確立の詳細は、上記実施の形態におけるSAC確立処理と同様であって、上記実施の形態において、端末10が行っていた処理を、ICメモリカードが行う。なお、ここで行うSAC確立処理の公開鍵暗号のアルゴリズムには、楕円曲線暗号を用いるとする。

**【0184】**

制御部は、サーバ装置30との間で確立されたSACを用いて、端末を介してサーバ装置30から暗号化コンテンツを受信し、受信した暗号化コンテンツを復号し、復号したコンテンツを記憶領域に格納する。

次に、ICメモリカードが、サーバ装置40に対してサービスの利用を要求するときの制御部の処理について説明する。制御部は、記憶領域からサービス用秘密鍵、公開鍵証明書（サーバ装置40から発行されたもの）、及び、サーバ装置40の公開鍵を読み出し、読み出したこれらの鍵情報を用いてサーバ装置40とSACを確立する。

**【0185】**

制御部は、サーバ装置40との間で確立されたSACを用いて、端末を介してサーバ装置40から暗号化コンテンツを受信し、受信した暗号化コンテンツを復号し、復号したコンテンツを記憶領域に格納する。

次に、ICメモリカードが、サーバ装置50に対してサービスの利用を要求するときの制御部の処理について説明する。制御部は、記憶領域からサービス用秘密鍵、公開鍵証明書（サーバ装置50から発行されたもの）、及び、サーバ装置50の公開鍵を読み出し、読み出したこれらの鍵情報を用いてサーバ装置50とSACを確立する。

**【0186】**

制御部は、サーバ装置50との間で確立されたSACを用いて、端末を介してサーバ装置50から暗号化コンテンツを受信し、受信した暗号化コンテンツを復号し、復号したコンテンツを記憶領域に格納する。

この様に、サーバ装置30、40、及び50から取得した各コンテンツは、当該ICメモリカードが挿入されている端末や、その他の端末により再生可能である。

**【0187】**

(8) 上記実施の形態では、CAがサーバ装置毎に異なるシステムパラメータを生成し、生成したシステムパラメータを、各サーバ装置へ送信する構成を有しているが、本発明において、サーバ装置は、必ずしもCAなどの外部からシステムパラメータを取得する必要はなく、サーバ装置自身がシステムパラメータを生成する構成であってもよい。

サーバ装置自身がシステムパラメータを生成する場合、サーバ装置毎に（業者毎に）異なる公開鍵が端末10で生成されるために、例えば、サーバ装置毎に異なるIDを割り当てて、各サーバ装置は、割り当てられたIDに基づきシステムパラメータを生成するように構成してもよい。

**【0188】**

(9) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読

み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0189】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0190】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(10) 上記実施の形態及び上記変形例をそれぞれ組み合わせる構成も本発明に含まれる。

【産業上の利用可能性】

【0191】

上記において説明した情報セキュリティシステムは、映画、音楽などのデジタル化された著作物を、放送やネットワークなどを介して流通させる産業において、ユーザが複数のサービス業者を利用する仕組みとして利用できる。

【図面の簡単な説明】

【0192】

【図1】 情報セキュリティシステム1の構成を示す図である。

【図2】 端末10の構成を機能的に示す機能ブロック図である。

【図3】 (a) パスワードテーブル120のデータ構成を示す図である。(b) CRL130のデータ構成を示す図である。

【図4】 メモリカード20の構成を機能的に示す機能ブロック図である。

【図5】 サーバ装置30の構成を機能的に示す機能ブロック図である。

【図6】 情報セキュリティシステム1全体の動作を示すフローチャートであり、図15に続く。

【図7】 端末10におけるメモリカード20の認証処理の動作を示すフローチャートである。

【図8】 認証局(CA)と各機器(端末10、サーバ装置30、サーバ装置40及びサーバ装置50)とにおける公開鍵証明書発行処理の動作を示すフローチャートである。

【図9】 (a) 公開鍵証明書140(Cert\_\_0010)のデータ構成を示す図である。(b) 公開鍵証明書150(Cert\_\_0030)のデータ構成を示す図である。(c) 公開鍵証明書160(Cert\_\_0040)のデータ構成を示す図である。(d) 公開鍵証明書170(Cert\_\_0050)のデータ構成を示す図である。

【図10】 端末10と各サーバ装置とにおけるサービス加入、登録処理の動作を示すフローチャートであり、図11に続く。

【図11】 端末10と各サーバ装置とにおけるサービス加入、登録処理の動作を示すフローチャートであり、図10から続く。

【図12】 (a) 端末10がサーバ装置30から発行される公開鍵証明書210(Cert\_\_A)のデータ構成を示す図である。(b) 端末10がサーバ装置40から発行される公開鍵証明書220(Cert\_\_B)のデータ構成を示す図である。(c) 端末10がサーバ装置50から発行される公開鍵証明書230(Cert\_\_C)のデータ構成を示す図である。

【図 1 3】 端末 1 0 と各サーバ装置とにおける、サービス加入、登録時の S A C 確立処理の動作を示すフローチャートであり、図 1 4 に続く。

【図 1 4】 端末 1 0 と各サーバ装置とにおける、サービス加入、登録時の S A C 確立処理の動作を示すフローチャートであり、図 1 3 から続く。

【図 1 5】 情報セキュリティシステム 1 全体の動作を示すフローチャートであり、図 6 から続く。

【図 1 6】 端末 1 0 と各サーバ装置とにおける、サービス利用時の S A C 確立処理の動作を示すフローチャートであり、図 1 7 に続く。

【図 1 7】 端末 1 0 と各サーバ装置とにおける、サービス利用時の S A C 確立処理の動作を示すフローチャートであり、図 1 6 から続き、図 1 8 へ続く。

【図 1 8】 端末 1 0 と各サーバ装置とにおける、サービス利用時の S A C 確立処理の動作を示すフローチャートであり、図 1 7 から続く。

【図 1 9】 認証局における楕円曲線のシステムパラメータ生成の動作を示すフローチャートである。

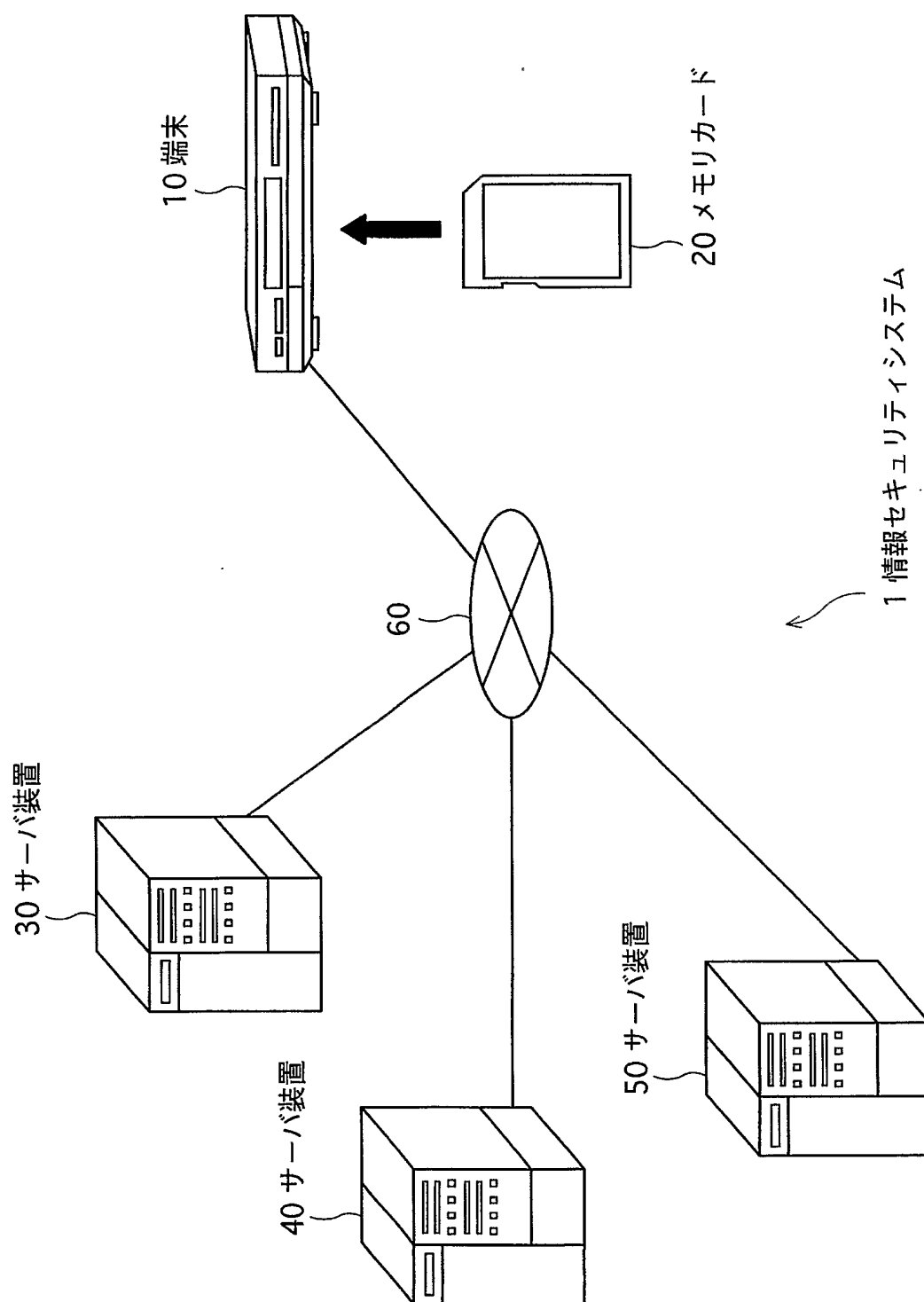
【符号の説明】

【 0 1 9 3 】

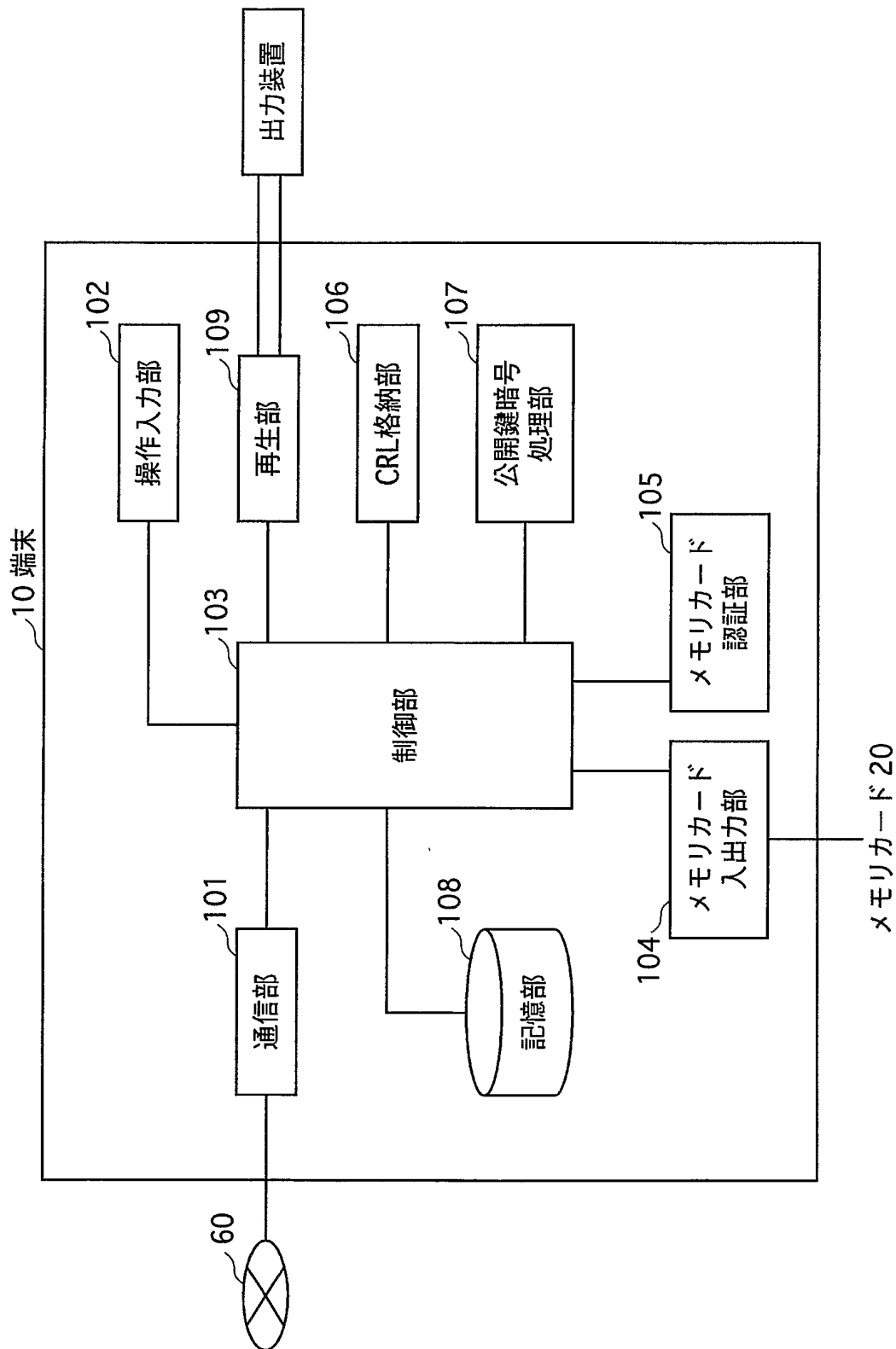
- 1 情報セキュリティシステム
- 1 0 端末
- 2 0 メモリカード
- 3 0 サーバ装置
- 4 0 サーバ装置
- 5 0 サーバ装置
- 6 0 ネットワーク
- 1 0 1 通信部
- 1 0 2 操作入力部
- 1 0 3 制御部
- 1 0 4 メモリカード入出力部
- 1 0 5 メモリカード認証部
- 1 0 6 C R L 格納部
- 1 0 7 公開鍵暗号処理部
- 1 0 8 記憶部
- 1 0 9 再生部
- 2 0 1 入出力部
- 2 0 2 メモリ制御部
- 2 0 3 認証部
- 2 0 4 メモリ
- 2 0 4 a セキュア領域
- 2 0 4 b コンテンツ格納領域
- 2 0 4 c 公開鍵格納領域
- 3 0 1 通信部
- 3 0 2 制御部
- 3 0 3 C R L 格納部
- 3 0 4 C e r t 管理部
- 3 0 5 登録情報管理部
- 3 0 6 公開鍵暗号処理部
- 3 0 7 コンテンツ格納部

【書類名】 図面

【図 1】



【図 2】





【図 3】

(a)

120 パスワードテーブル

メモリカード番号	認証用パスワード
20	PW_0
21	PW_1
⋮	⋮

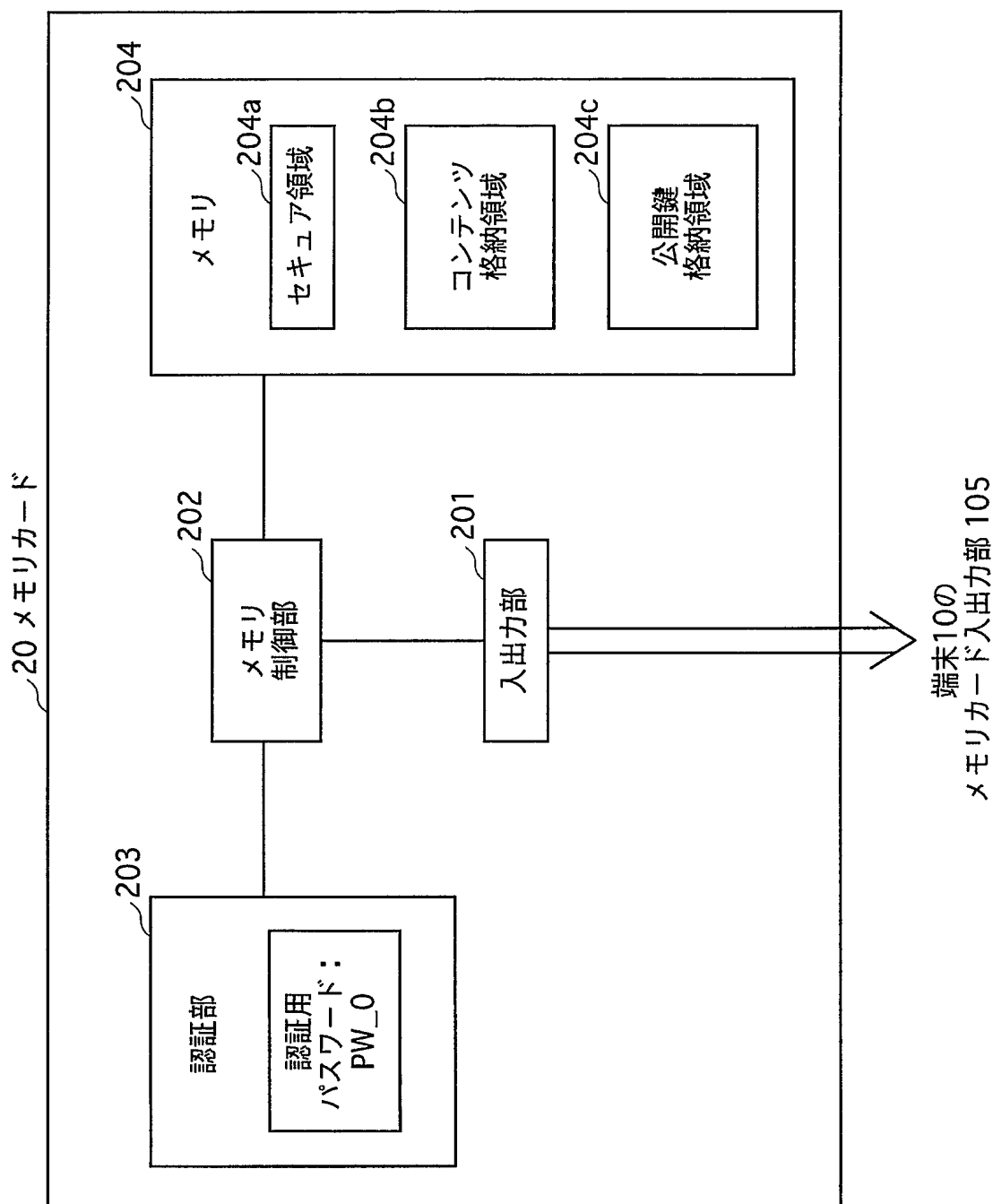
121

(b)

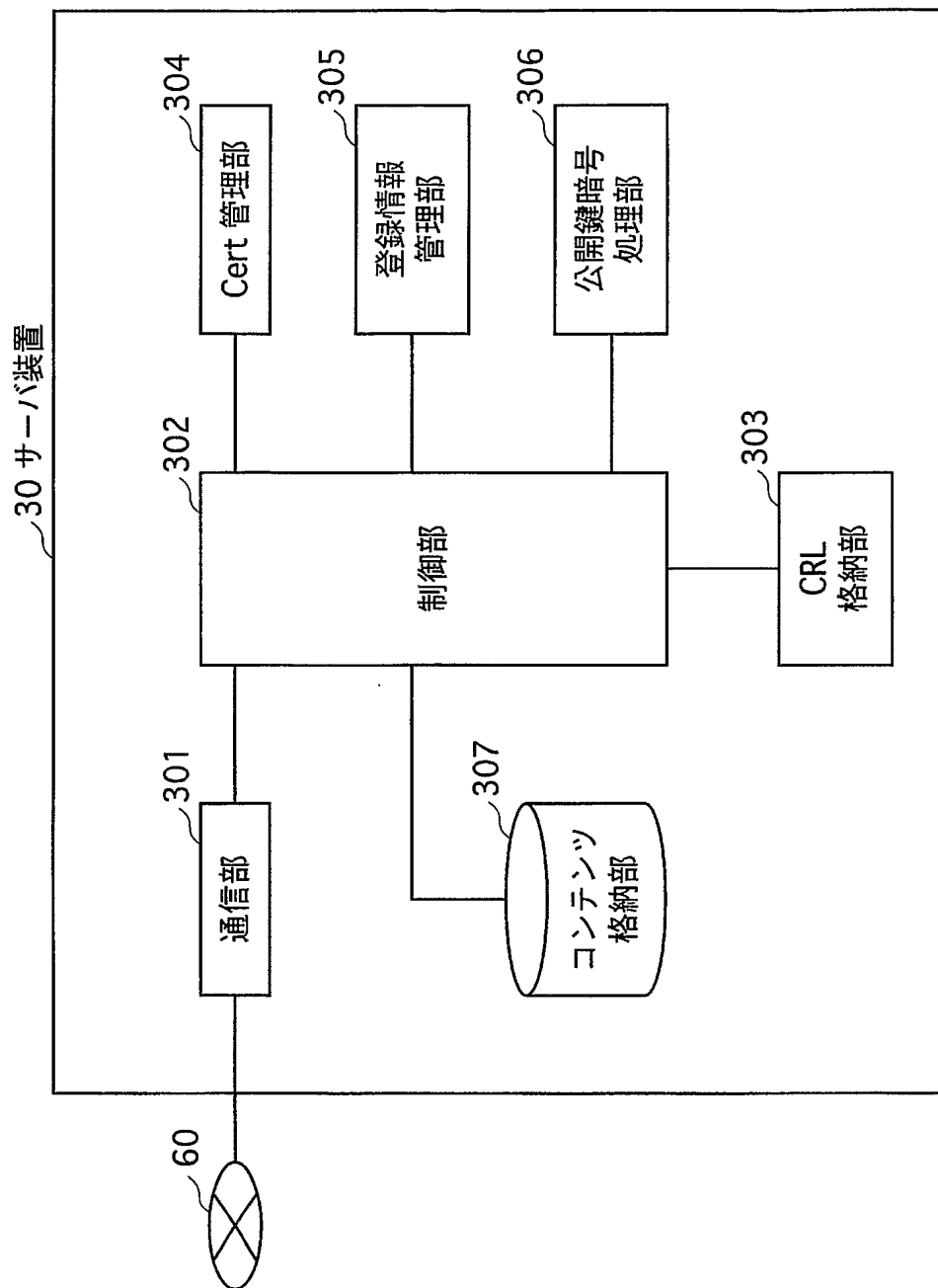
130 CRL

無効化された機器のID
ID_0012
ID_0058
ID_0379
⋮

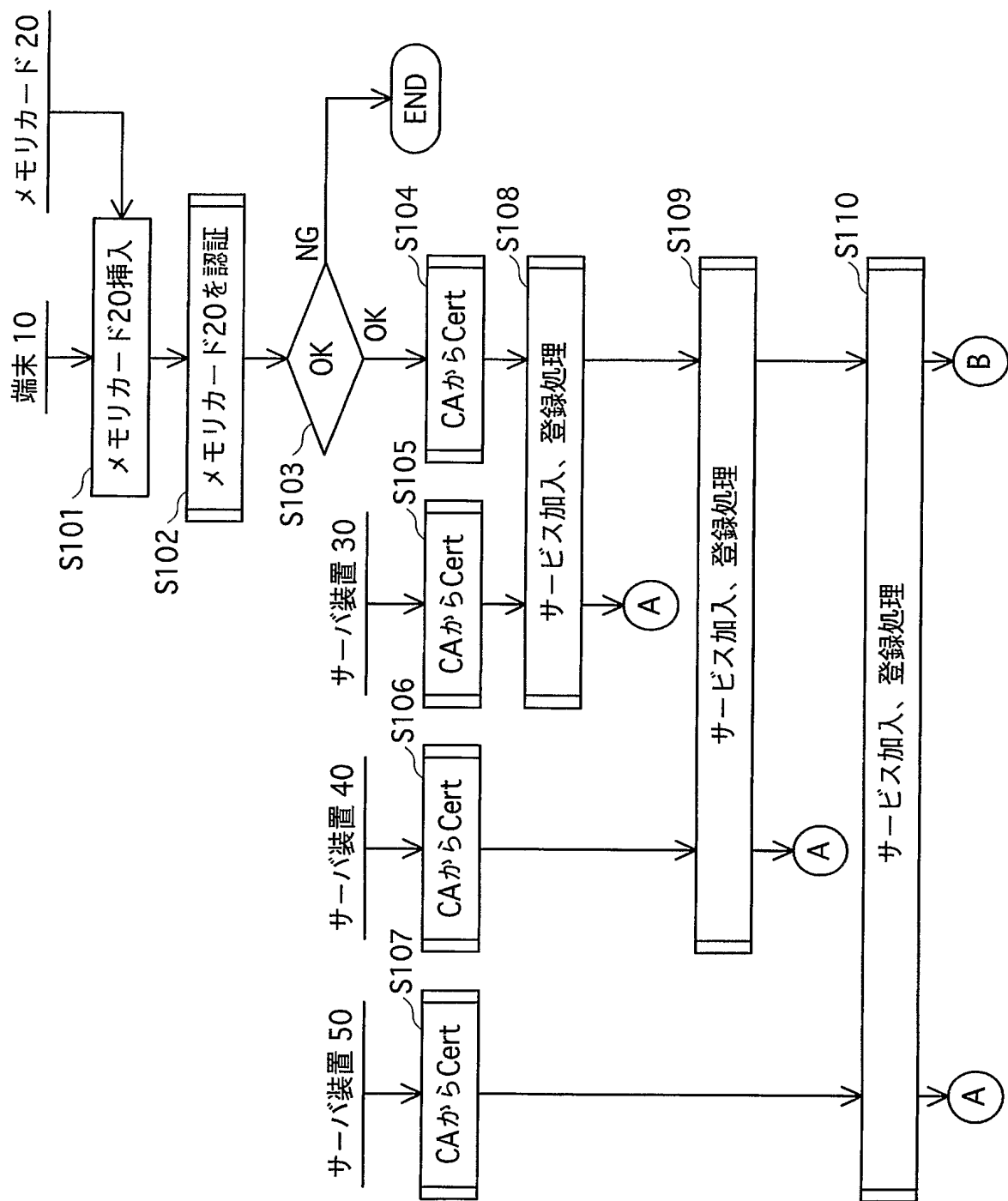
【図 4】



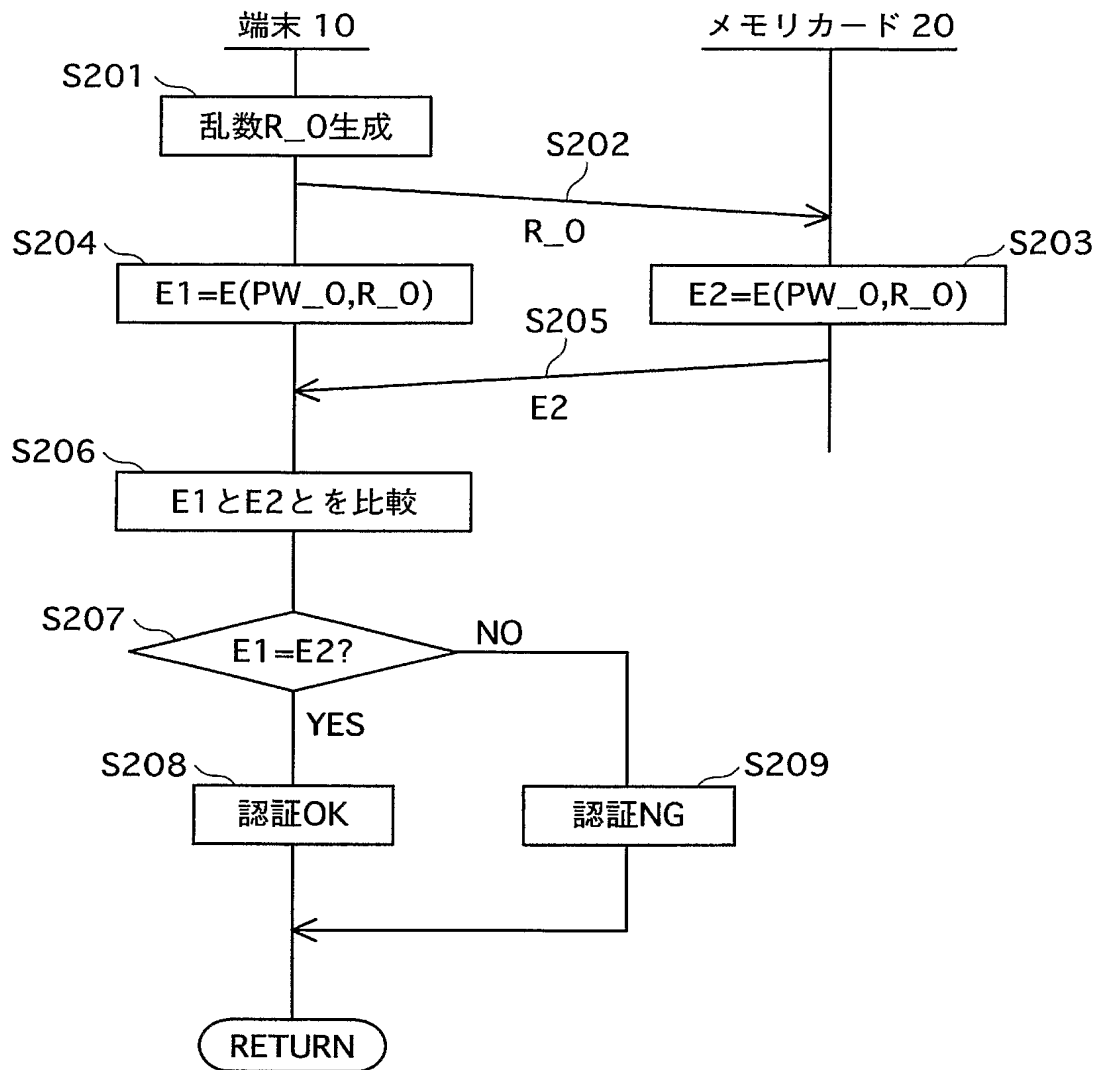
【図 5】



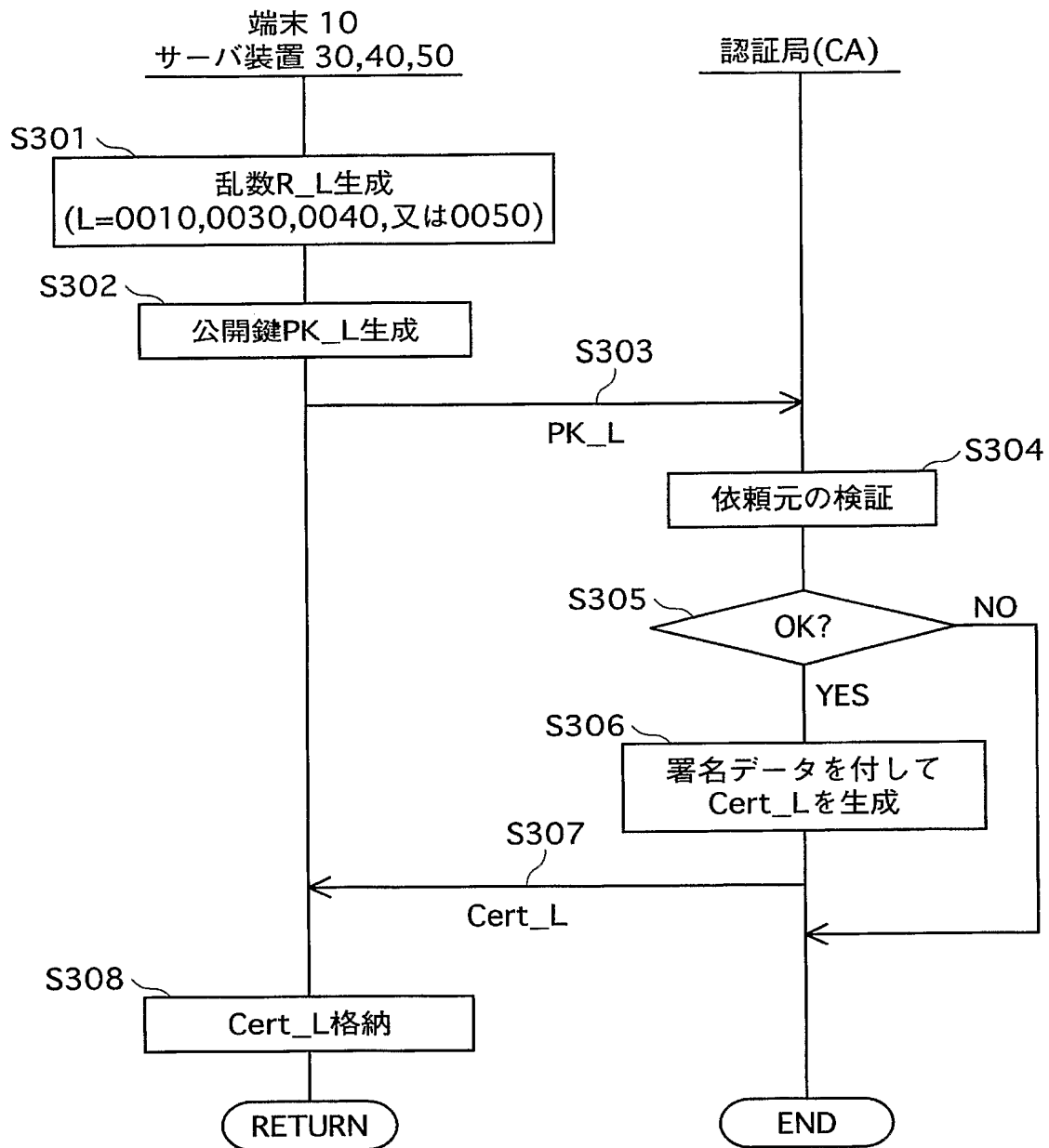
【図 6】



【図 7】



【図 8】



【図 9】

(a) CAから発行される端末 10の公開鍵証明書

ID_0010	↙ 140 Cert_0010
PK_0010	
Sig_0010CA	

(b) CAから発行されるサーバ装置 30の公開鍵証明書

ID_0030	↙ 150 Cert_0030
PK_0030	
Sig_0030CA	

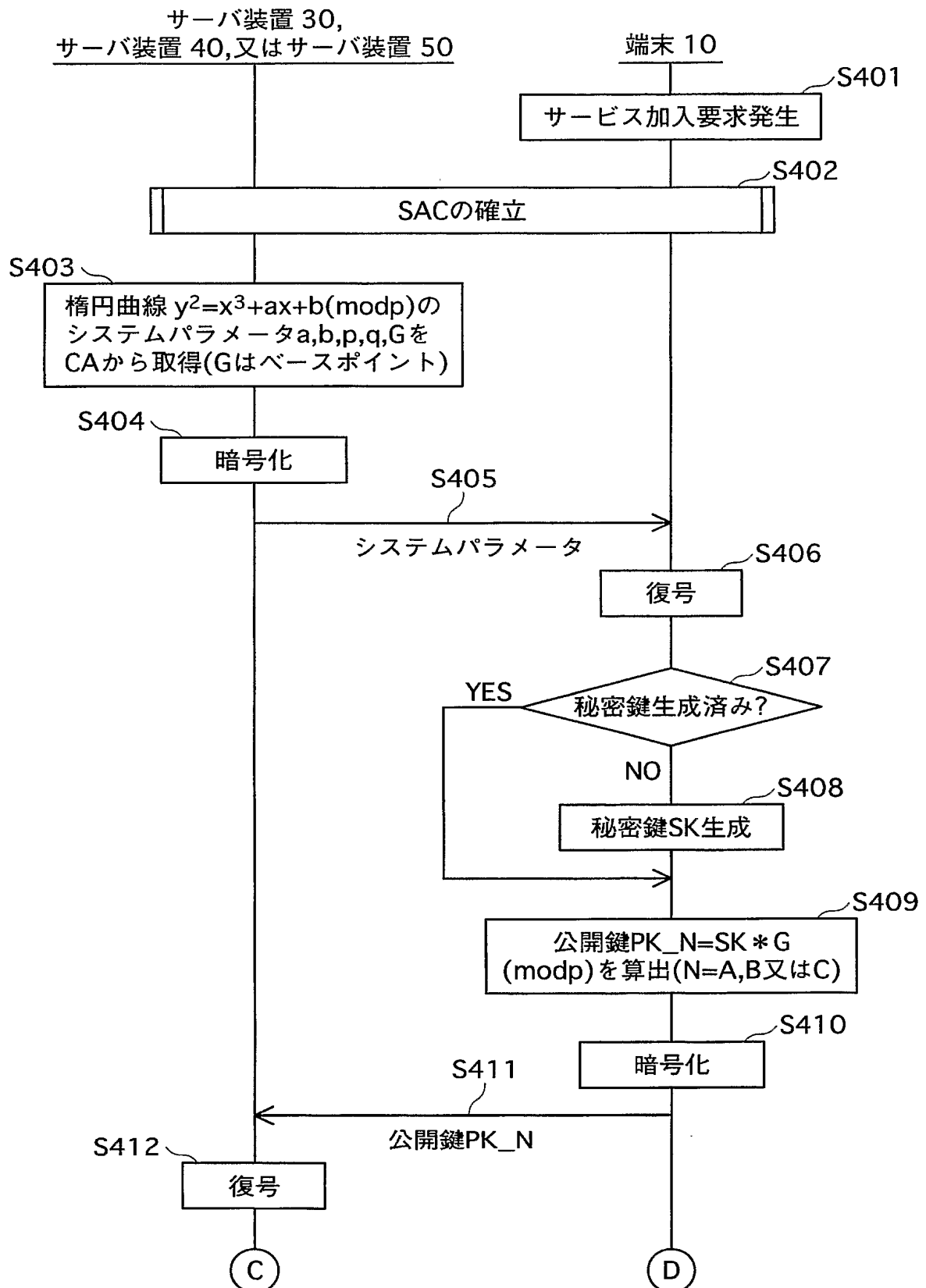
(c) CAから発行されるサーバ装置 40の公開鍵証明書

ID_0040	↙ 160 Cert_0040
PK_0040	
Sig_0040CA	

(d) CAから発行されるサーバ装置 50の公開鍵証明書

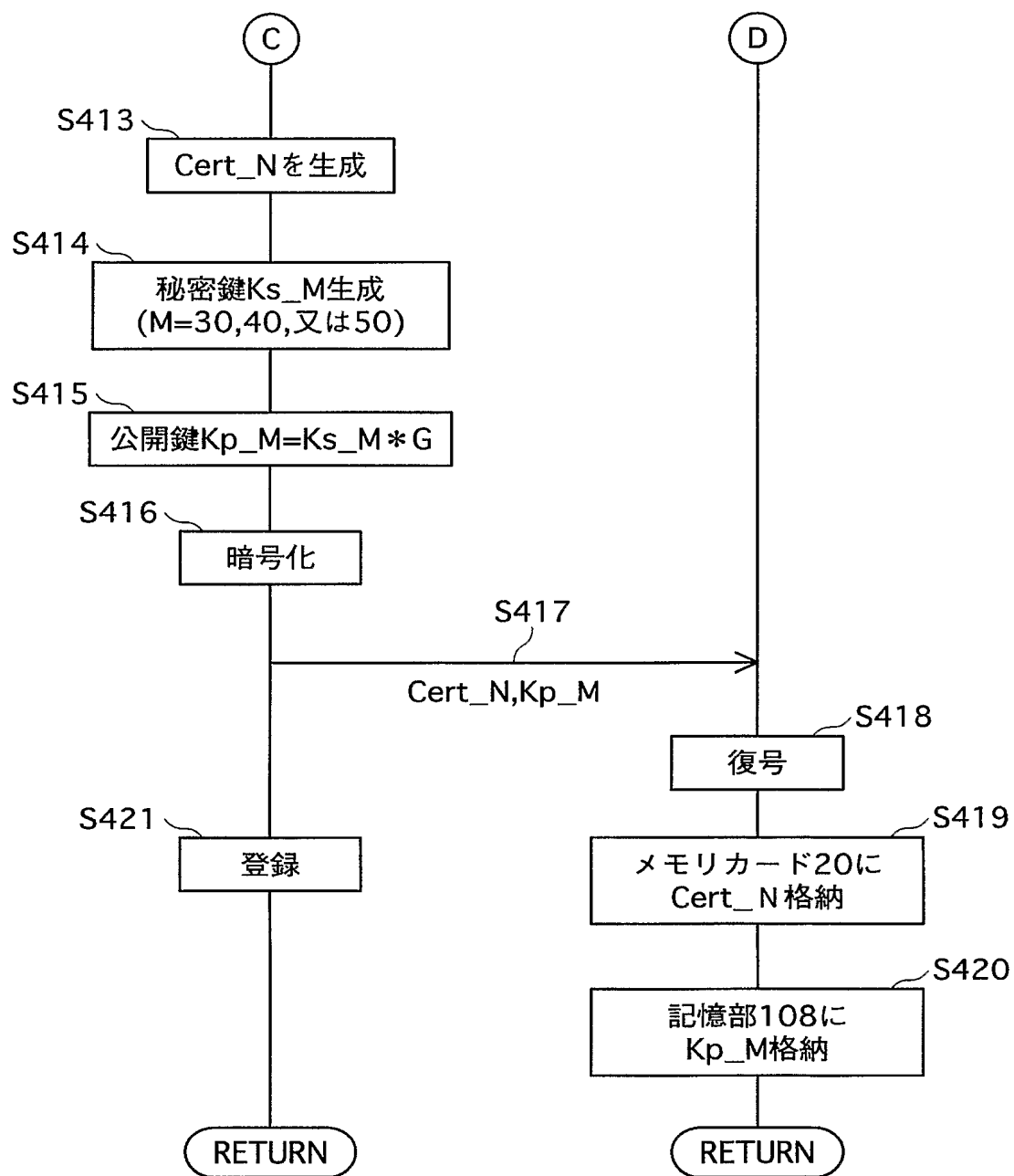
ID_0050	↙ 170 Cert_0050
PK_0050	
Sig_0050CA	

【図 10】





【図 11】



【図 12】

(a) サーバ装置 30 から発行される公開鍵証明書

サービスID	SID_0123A
会員番号	NO_0001
公開鍵	PK_A
署名データ	Sig_A

210 Cert\_A

(b) サーバ装置 40 から発行される公開鍵証明書

サービスID	SID_0321B
会員番号	NO_0025
公開鍵	PK_B
署名データ	Sig_B

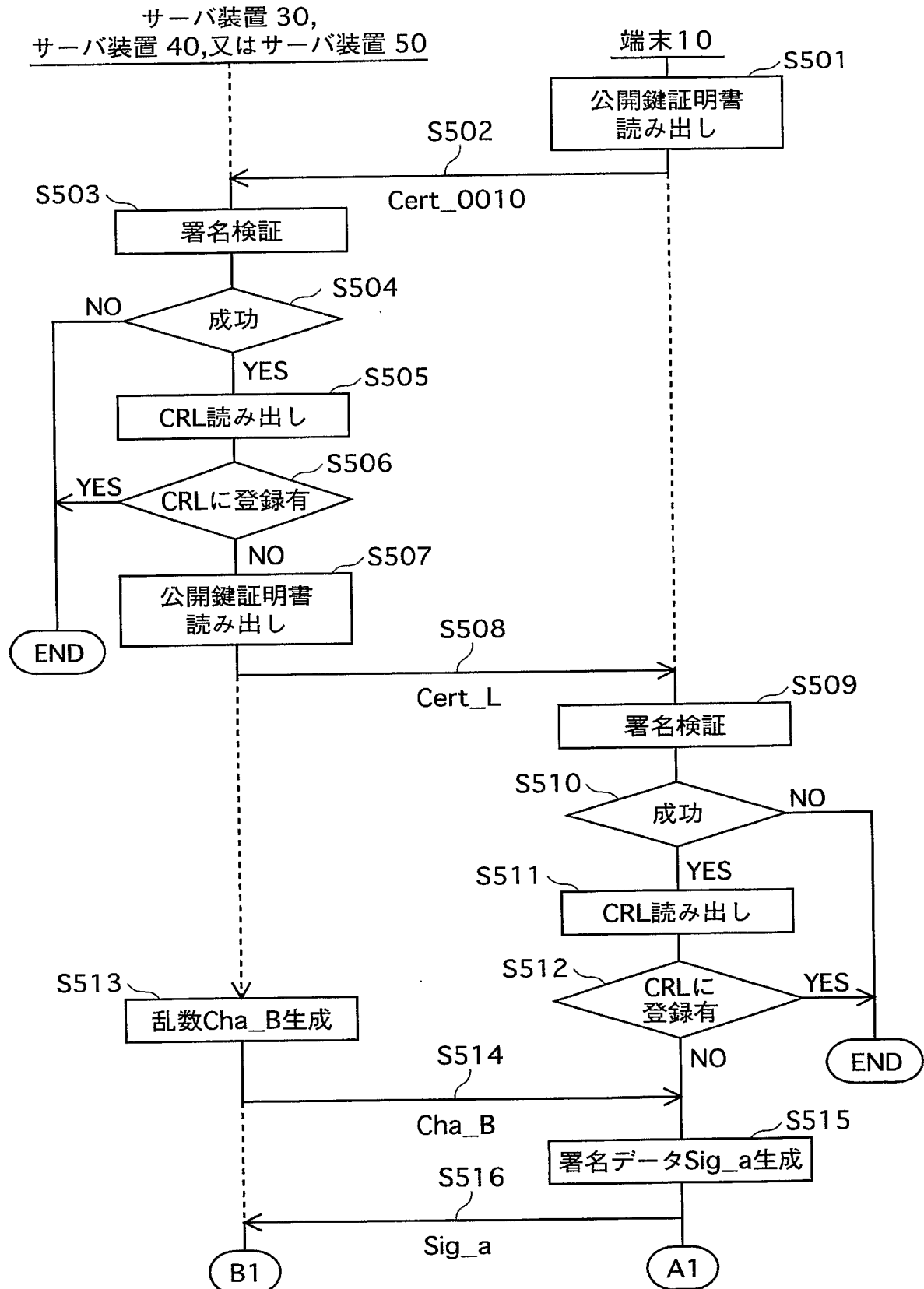
220 Cert\_B

(c) サーバ装置 50 から発行される公開鍵証明書

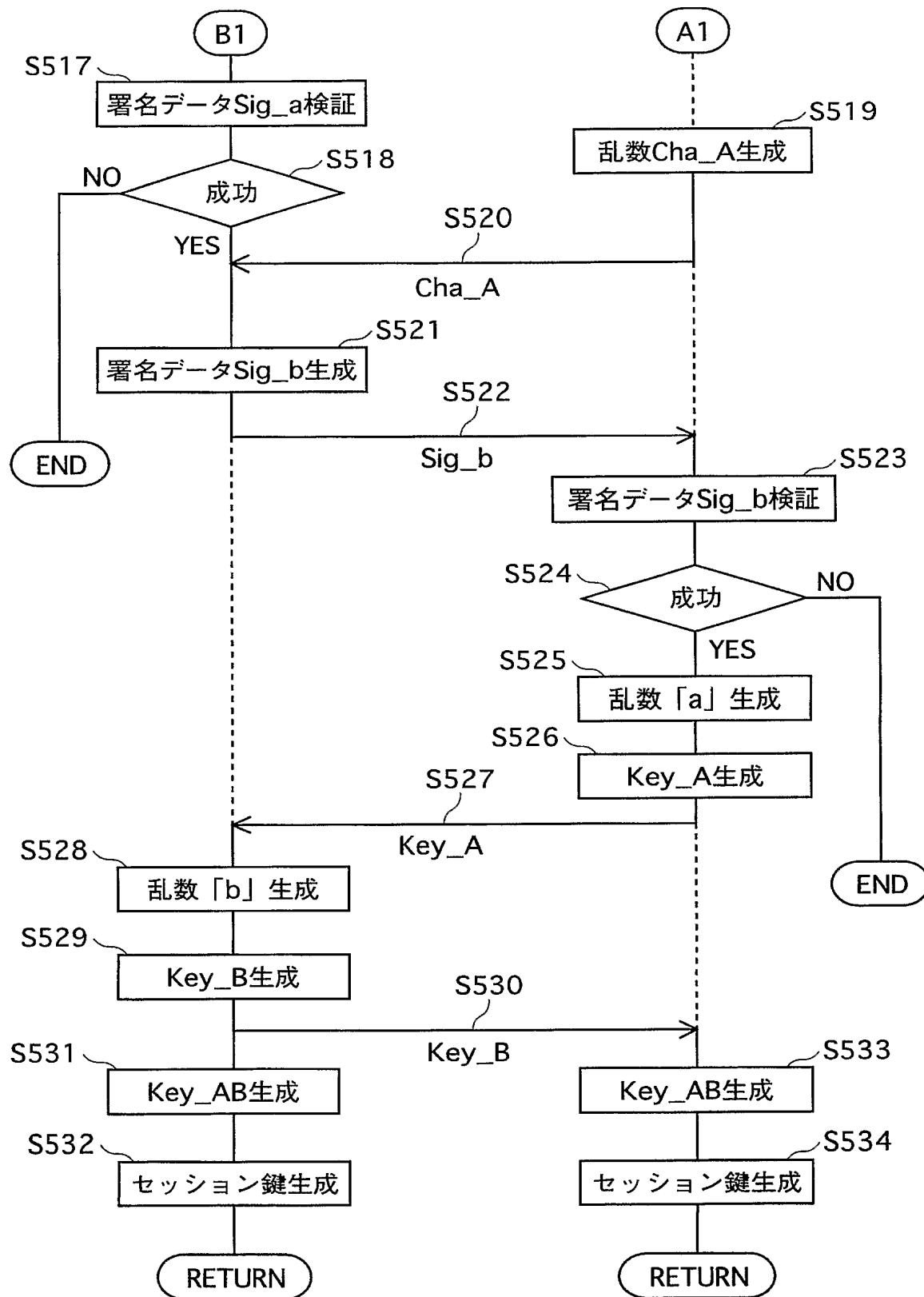
サービスID	SID_0132C
会員番号	NO_3215
公開鍵	PK_C
署名データ	Sig_C

230 Cert\_C

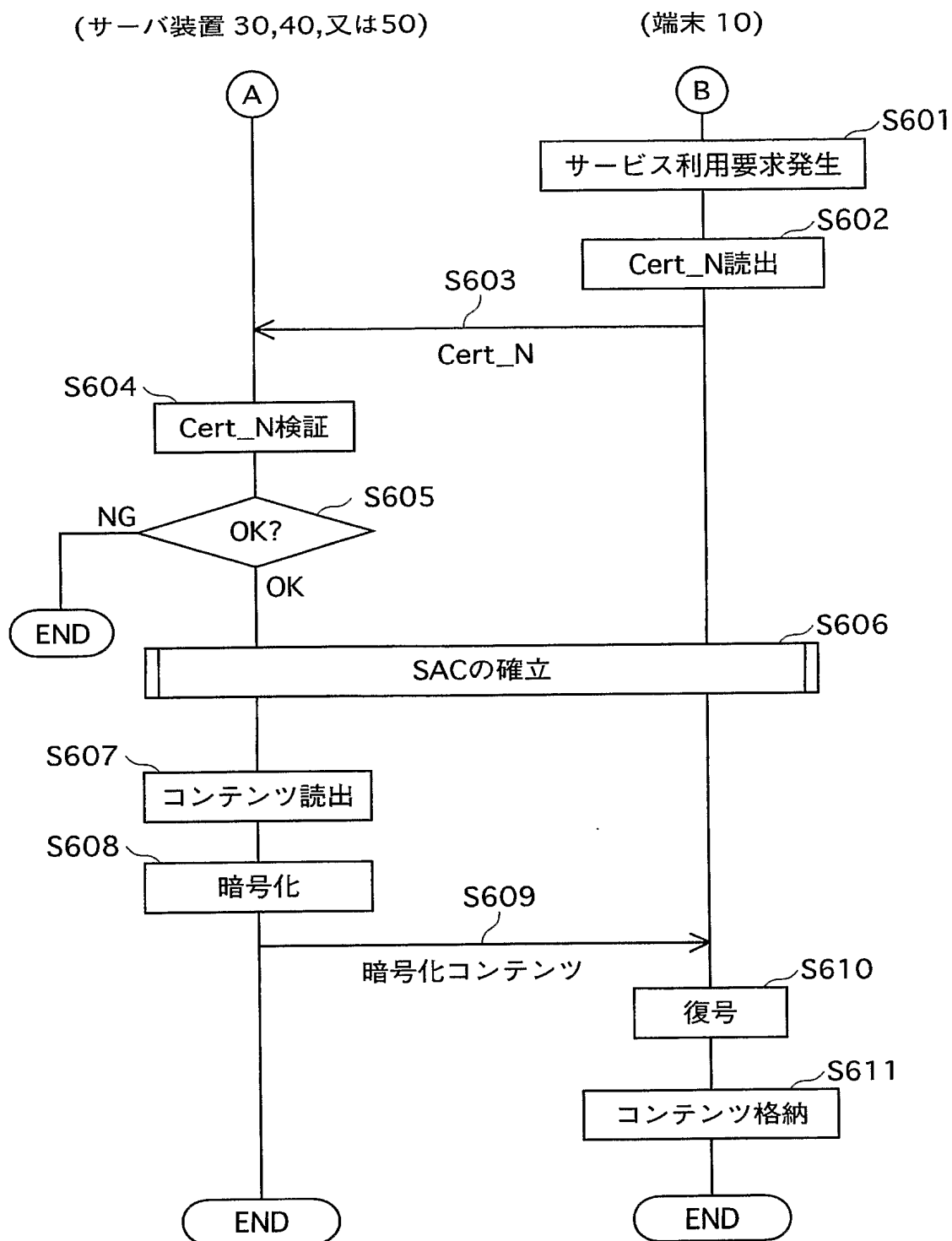
【図 13】



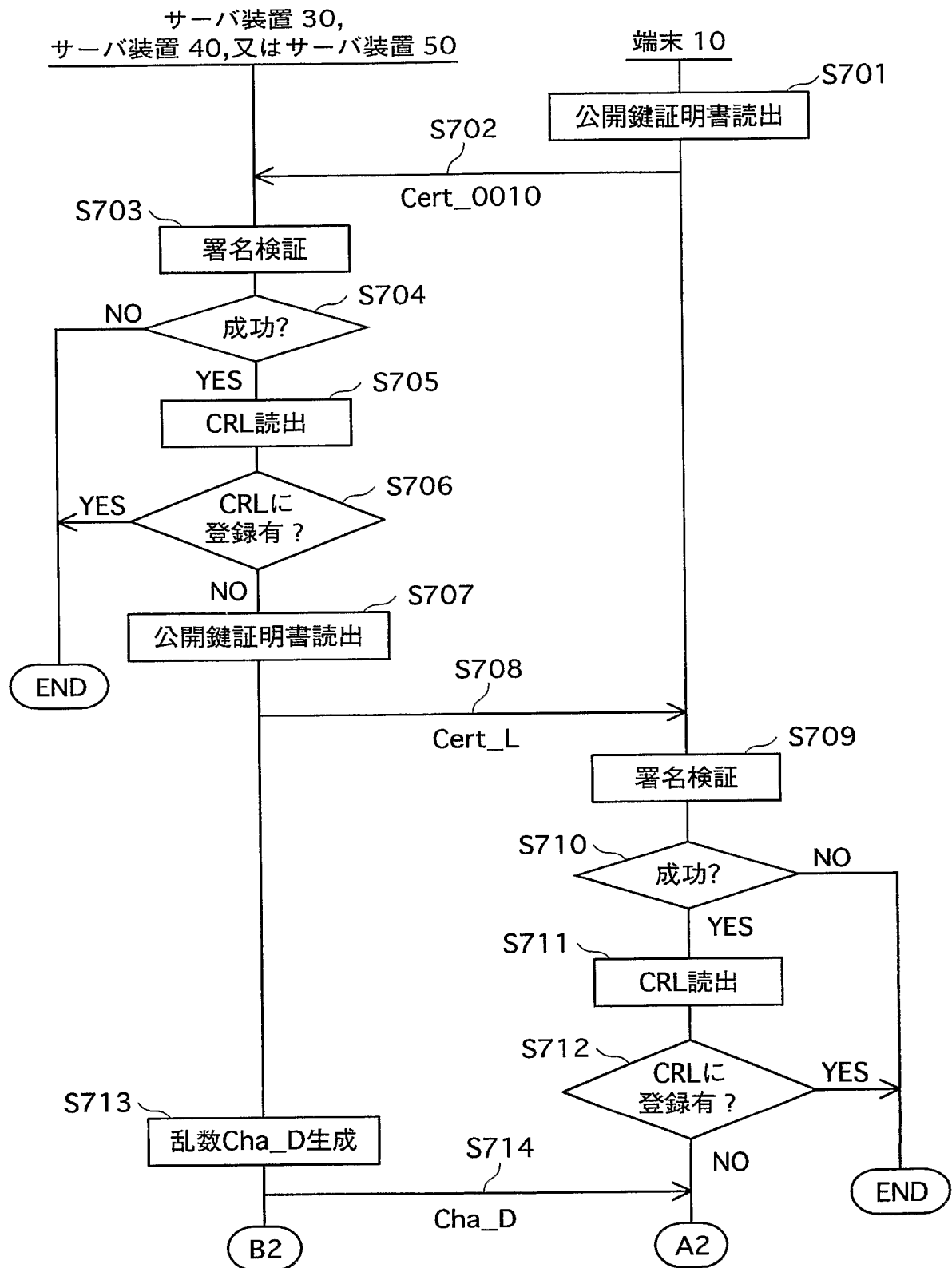
【図 14】



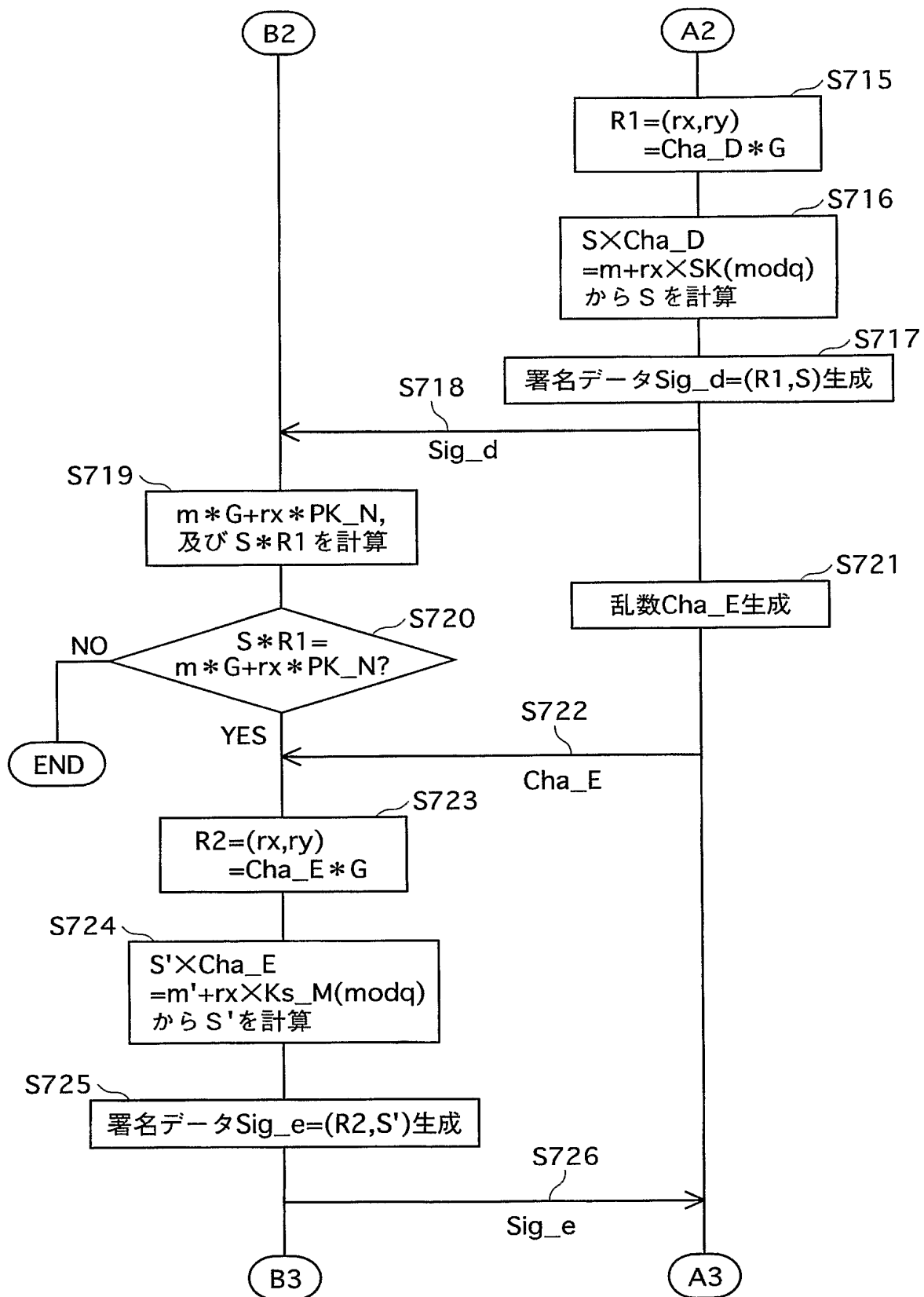
【図15】



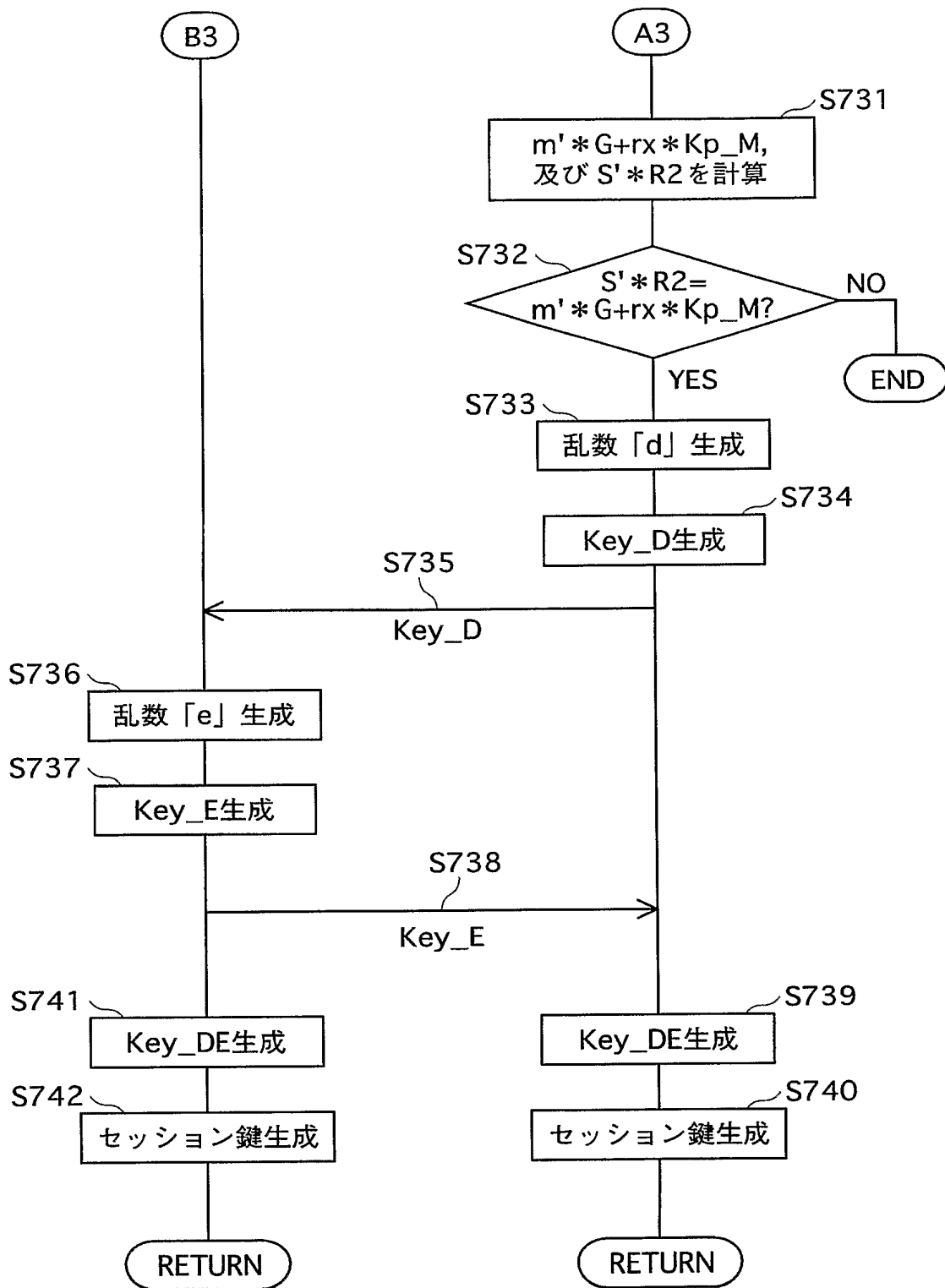
【図 16】



【図 17】

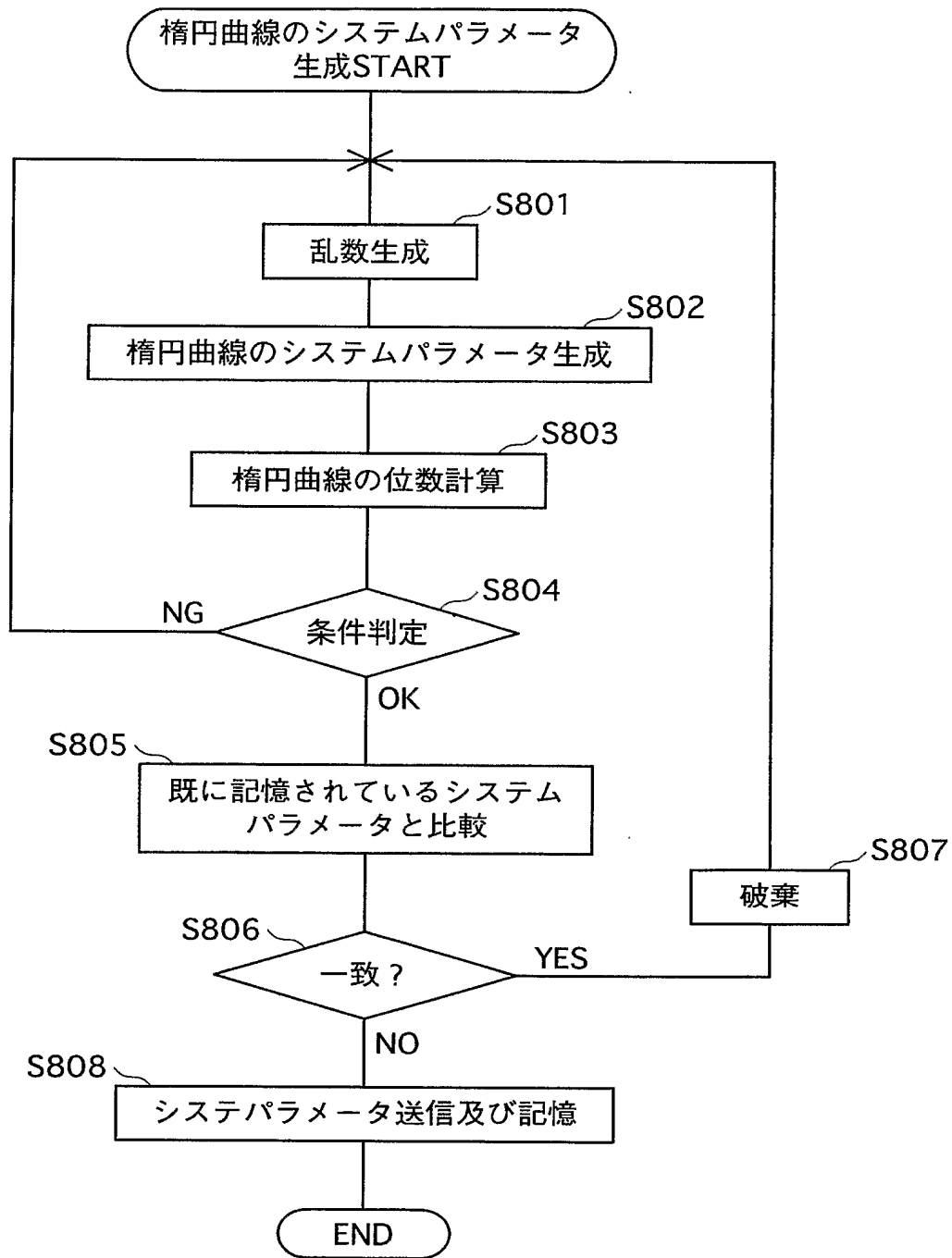


【図 18】





【図 19】



【書類名】要約書

【要約】

【課題】 1 台の端末で複数業者のサービスを利用するのに適した情報セキュリティ装置及び情報セキュリティシステムを提供することを目的とする

【解決手段】 同一の条件を有する整数の集合上で、一の演算の逆算を行うことが計算量上困難であることを利用して、情報を安全かつ確実に扱う情報セキュリティ装置であって、秘密鍵を生成する秘密鍵生成手段と、前記条件を特定するパラメータを複数取得するパラメータ取得手段と、取得した複数のパラメータによりそれぞれ決定される複数の集合上で、前記秘密鍵を用いて、複数の公開鍵を生成する公開鍵生成手段とを備えることを特徴とする。

【選択図】 図 1

特願 2 0 0 4 - 0 7 4 7 3 9

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社